No. 16-402	
Title:	**Timothy Ivory Carpenter, Petitioner** **v.** **United States**
Docketed:	September 28, 2016
Lower Ct:	United States Court of Appeals for the Sixth Circuit
Case Numbers:	(14-1572)
Decision Date:	April 13, 2016
Rehearing Denied:	June 29, 2016
Questions Presented	

DATE	PROCEEDINGS AND ORDERS
Sep 26 2016	Petition for a writ of certiorari filed. (Response due October 28, 2016)
Oct 21 2016	Order extending time to file response to petition to and including November 28, 2016.
Oct 28 2016	Brief amici curiae of Electronic Frontier Foundation, et al. filed.
Oct 28 2016	Brief amicus curiae of Cato Institute filed.
Nov 21 2016	Order further extending time to file response to petition to and including December 28, 2016.
Dec 15 2016	Order further extending time to file response to petition to and including January 27, 2016.
Jan 27 2017	Brief of respondent United States in opposition filed.
Feb 10 2017	Reply of petitioner Timothy Ivory Carpenter filed.
Feb 15 2017	DISTRIBUTED for Conference of March 3, 2017.
Feb 23 2017	Rescheduled.

Mar 22 2017	DISTRIBUTED for Conference of April 13, 2017.
Apr 17 2017	DISTRIBUTED for Conference of April 21, 2017.
Apr 24 2017	DISTRIBUTED for Conference of April 28, 2017.
May 08 2017	DISTRIBUTED for Conference of May 11, 2017.
May 15 2017	DISTRIBUTED for Conference of May 18, 2017.
May 22 2017	DISTRIBUTED for Conference of May 25, 2017.
May 30 2017	DISTRIBUTED for Conference of June 1, 2017.
Jun 05 2017	Petition GRANTED.
Jun 22 2017	The time to file the joint appendix and petitioner's brief on the merits is extended to and including August 7, 2017.
Jun 22 2017	The time to file respondent's brief on the merits is extended to and including September 25, 2017.
Jul 11 2017	Consent to the filing of amicus curiae briefs in support of either party or neither party received from counsel for the petitioner.
Jul 12 2017	Motion for leave to proceed further herein in forma pauperis filed by petitioner Timothy I. Carpenter.
Jul 12 2017	Motion to appoint counsel filed by petitioner Timothy I. Carpenter.
Jul 26 2017	Consent to the filing of amicus curiae briefs in support of either or neither party received from counsel for the respondent.
Aug 02 2017	DISTRIBUTED for Conference of 9/25/2017.
Aug 07 2017	Joint appendix filed.
Aug 07 2017	Brief of petitioner Timothy I. Carpenter filed.
Aug 11 2017	Brief amici curiae of Data & Society Research Institute and Fifteen scholars of Technology and Society filed.

Aug 11 2017	Brief amici curiae of Competitive Enterprise Institute, et al. filed.
Aug 14 2017	Brief amicus curiae of Center for Democracy and Technology filed.
Aug 14 2017	Brief amici curiae of Empirical Fourth Amendment Scholars filed.
Aug 14 2017	Brief amici curiae of Electronic Privacy Information Center, et al. filed.
Aug 14 2017	Brief amicus curiae of The Rutherford Institute filed.
Aug 14 2017	Brief amici curiae of The Center for Competitive Politics, et al. filed.
Aug 14 2017	Brief amici curiae of Scholars of the History and Original Meaning of the Fourth Amendment filed.
Aug 14 2017	Brief amici curiae of The Reporters Committee for Freedom of the Press, et al. filed.
Aug 14 2017	Brief amici curiae of Technology Companies in support of neither party filed.
Aug 14 2017	Brief amici curiae of Scholars of Criminal Procedure and Privacy filed.
Aug 14 2017	Brief amici curiae of Electronic Frontier Foundation, et al. filed.
Aug 14 2017	Brief amici curiae of Institute for Justice, et al. filed.
Aug 14 2017	Brief amicus curiae of Restore the Fourth, Inc. filed.
Aug 14 2017	Brief amici curiae of United States Justice Foundation, et al. filed.
Aug 14 2017	Brief amici curiae of Technology Experts filed.
Sep 25 2017	Brief of respondent United States filed.
Sep 29 2017	Brief amicus curiae of Michael Varco filed.
Oct 02 2017	Motion for leave to proceed further herein in forma pauperis granted by the Court

Oct 02 2017	Motion to appoint counsel filed by petitioner GRANTED and Harold Gurewitz, Esquire, of Detroit, Michigan, is appointed to serve as counsel for the petitioner in this case.
Oct 02 2017	Brief amici curiae of Alabama, et al. filed.
Oct 02 2017	Brief amicus curiae of Professor Orin S. Kerr filed.
Oct 02 2017	Brief amicus curiae of National District Attorneys Association filed.
Oct 06 2017	SET FOR ARGUMENT ON Wednesday, November 29, 2017
Oct 12 2017	CIRCULATED
Oct 18 2017	Record requested from the U.S.C.A. 6th Circuit.
Oct 23 2017	Record received from the U.S.C.A. 6th Circuit is electronic.
Oct 24 2017	Reply of petitioner Timothy I. Carpenter filed. (Distributed)
Nov 29 2017	Argued. For petitioner: Nathan F. Wessler, New York, N. Y. For respondent: Michael R. Dreeben, Deputy Solicitor General, Department of Justice, Washington, D. C.

NAME	ADDRESS	PHONE
Attorneys for Petitioner		
Harold Gurewitz Counsel of Record	Gurewitz and Raben, PLC 333 West Fort St., Suite 1400 Detroit, MI 48226 hgurewitz@grplc.com	313-628-4733
Party name: Timothy I. Carpenter		
Nathan F. Wessler	ACLU Foundation 125 Broad Street New York, NY 10004 nwessler@aclu.org	(212) 549-2500
Party name: Timothy Ivory Carpenter		
Attorneys for Respondent		
Noel J. Francisco	Solicitor General	202-514-2217

Counsel of Record	United States Department of Justice 950 Pennsylvania Avenue, NW Washington, DC 20530-0001 SupremeCtBriefs@USDOJ.gov	
Party name: United States		

Other

Amitabh Agarwal Counsel of Record	Office of the Attorney General PL-1, The Capitol Tallahassee, FL 32399 Amit.Agarwal@myfloridalegal.com	(850) 414-3000
Party name: The States of Alabama, et al.		
John M. Castellano Counsel of Record	125-01 Queens Boulevard Kew Gardens, NY 11415 jmcastellano@queensda.org	718-286-5801
Party name: National District Attorneys Association		
Andrew Gellis Crocker Counsel of Record	Electronic Frontier Foundation 815 Eddy Street San Francisco, CA 94109 andrew@eff.org	415-436-9333
Party name: Electronic Frontier Foundation, et al.		
James W. Harper Counsel of Record	Competitive Enterprise Institute 1310 L St., NW, 7th Fl. Washington, DC 20005 jim.harper@cei.org	202-331-1010
Party name: Competitive Enterprise Institute, et al.		
Dorothy Alicia Hickok Counsel of Record	Drinker Biddle & Reath LLP One Logan Square Philadelphia, PA 19103 alicia.hickok@dbr.com	(215)-988-2700
Party name: The Rutherford Institute		
Wesley Patrick Hottot Counsel of Record	Institute for Justice 10500 Northeast 8th St., Suite 1760 Bellevue, WA 98004 whottot@ij.org	425-646-9300
Party name: Institute for Justice, et al.		
Orin S. Kerr Counsel of Record	2000 H Street, NW Washington, DC 20052 okerr@law.gwu.edu	(202) 994-4775

Party name: Professor Orin S. Kerr

Robert Jeffrey Olson Counsel of Record	William J. Olson, P.C. 370 Maple Avenue West, Suite 4 Vienna, VA 22180-5615 wjo@mindspring.com	703-356-5070

Party name: United States Justice Foundation, et al.

Andrew John Pincus Counsel of Record	Mayer Brown LLP 1999 K Street, NW Washington, DC 20006 apincus@mayerbrown.com	(202) 263-3000

Party name: Center for Democracy & Technology

Marc Rotenberg Counsel of Record	Electronic Privacy Information Center (EPIC) 1718 Connecticut Ave., NW Suite 200 Washington, DC 20009 rotenberg@epic.org	202-483-1140

Party name: Electronic Privacy Information Center, et al.

Harry Sandick Counsel of Record	Patterson Belknap Webb & Tyler LLP 1133 Avenue of the Americas New York, NY 10036 hsandick@pbwt.com	(212) 336-2000

Party name: Scholars of Criminal Procedure and Privacy

Sarah O'Rourke Schrup Counsel of Record	Northwestern Supreme Court Practicum 357 East Chicago Ave. Chicago, IL 60611 s-schrup@law.northwestern.edu	(312)-503-0063

Party name: Empirical Fourth Amendment Scholars

Andrew David Selbst Counsel of Record	Data & Society Research Institute 36 W. 20th Street, 11th Fl. New York, NY 10011 andrew@datasociety.net	617-504-1982

Party name: Data & Society Research Institute and fifteen scholars of technology and society

Mahesha Padmanabhan Subbaraman Counsel of Record	Subbaraman PLLC 222 S. 9th St., Suite 1600 Minneapolis, MN 55402 mps@subblaw.com	612-315-9210

Party name: Restore the Fourth, Inc.

Michael Anthony Varco Counsel of Record	P.O. Box 2548 Reston, VA 20195	703-635-7903

m_varco@yahoo.com

Party name: Michael Varco

Seth P. Waxman Counsel of Record	Wilmer Cutler Pickering Hale and Dorr LLP 1875 Pennsylvania Ave, NW Washington, DC 20006 seth.waxman@w...nerhale.com	(202) 663-6000

Party name: Technology Companies in support of neither party

Alexander Abraham Abdo	Knight First Amendment Institute, Columbia University 535 West 116th Street 314 Low Library New York, NY 10027 alex.abdo@knightcolumbia.org	212-854-9600

Party name: Technology Experts

Gorod Brianne	Constitutional Accountability of the Fourth Amendment 1200 18th Street, NW Suite 501 Washington, DC 20036 brianne@theusconstition.org	292-296-6889

Party name: Scholars of History and Original Meaning of the Fourth Amendment

Bruce D. Brown	The Reporters Committee for Freedom of the Press 1156 15th St., NW Suite 1250 Washington, DC 20005 bbrown@rcfp.org	202-795-9300

Party name: The Reporters Committee for Freedom of the Press, et al.

Allen Joseph Dickerson	Center for Competitive Politics 124 S. West Street Suite 201 Alexandria, VA 22314 adickerson@campaignfreedom.org	(703)-894-6800

Party name: The Center for Competitive Politics, et al.

James W. Harper	Cato Institute 1000 Massachuetts Ave., N.W. Washington, DC 20001 jharper@cato.org	(202) 842-0200

Party name: Cato Institute

Jennifer Lynch	Electronic Frontier Foundation 815 Eddy Street	(415)-436-9333

San Francisco, CA 94109

jlynch@eff.org

Party name: Electronic Frontier Foundation, et al.

RECORD AND BRIEF

16-402

No. _____

FILED
SEP 26 2016
OFFICE OF THE CLERK

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

—v.—

UNITED STATES OF AMERICA,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
AMERICAN CIVIL LIBERTIES UNION FUND OF MICHIGAN
2966 Woodward Ave.
Detroit, MI 48201

Nathan Freed Wessler
Counsel of Record
Ben Wizner
Steven R. Shapiro
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

Harold Gurewitz
GUREWITZ & RABEN, PLC
333 W. Fort Street, Suite 1400
Detroit, MI 48226

QUESTION PRESENTED

In this case, as in thousands of cases each year, the government sought and obtained the historical cell phone location data of a private individual pursuant to a disclosure order under the Stored Communications Act (SCA) rather than by securing a warrant. Under the SCA, a disclosure order does not require a finding of probable cause. Instead, the SCA authorizes the issuance of a disclosure order whenever the government "offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

As a result, the district court never made a probable cause finding before ordering Petitioner's service provider to disclose months' worth of Petitioner's cell phone location records. A divided panel of the Sixth Circuit held that there is no reasonable expectation of privacy in these location records, relying in large part on four-decade-old decisions of this Court.

The Question Presented is:

Whether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 127 days is permitted by the Fourth Amendment.

PARTIES TO THE PROCEEDINGS

In addition to the parties named in the caption, Timothy Michael Sanders was a defendant-appellant below, and was represented by separate counsel.

TABLE OF CONTENTS

QUESTION PRESENTED i

PARTIES TO THE PROCEEDINGS ii

TABLE OF AUTHORITIES vi

PETITION FOR A WRIT OF CERTIORARI 1

OPINIONS BELOW 1

JURISDICTION 1

RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS 1

STATEMENT OF THE CASE 3

REASONS FOR GRANTING THE WRIT 10

I. THIS CASE PRESENTS AN IMPORTANT AND RECURRING QUESTION ON THE SCOPE OF CONSTITUTIONAL PRIVACY RIGHTS IN THE DIGITAL AGE 10

A. The Lower Courts Have Expressly and Repeatedly Sought This Court's Guidance in Addressing the Question Presented. ... 10

B. This Court's Recent Decisions Have Properly Recognized a Need to Reexamine Traditional Understandings of Privacy in the Digital Age 16

C. The Volume and Frequency of Warrantless Law Enforcement Requests for CSLI Highlights the Importance of the Question Presented. 18

II. FEDERAL COURTS OF APPEALS AND STATE HIGH COURTS ARE DIVIDED. 21

A. The Circuits Are Split Over Whether the Third-Party Doctrine Eliminates People's Reasonable Expectation of Privacy in Their Historical CSLI. 21

B. The Circuits Are Split Over Whether There is a Reasonable Expectation of Privacy in Longer-Term Location Information Collected by Electronic Means. 24

III. THE SIXTH CIRCUIT ERRED IN HOLDING THAT THE CONDUCT HERE WAS NOT A SEARCH 26

A. The Sixth Circuit Erred in Holding That There Is No Reasonable Expectation of Privacy in Historical CSLI. 26

B. The Sixth Circuit Erred In Deferring to Congress's 30-Year-Old Legislative Scheme. 32

CONCLUSION 35

APPENDIX 1a

Opinion, United States Court of Appeals for the Sixth Circuit (April 13, 2016) 1a

Order, United States Court of Appeals for the Sixth Circuit (June 29, 2016) 33a

Opinion & Order, United States District Court, Eastern District Of Michigan, Southern Division (Dec. 6, 2013) 34a

Application, United States District Court, Eastern District Of Michigan, Southern Division (May 2, 2011) 49a

Order, United States District Court, Eastern District of Michigan, Southern Division (May 2, 2011) 56a

Application, United States District Court, Eastern District of Michigan, Southern Division (June 7, 2011) 62a

Order, United States District Court, Eastern District of Michigan, Southern Division (June 7, 2011) 69a

Government Trial Exhibit 57, Federal Bureau Of Investigation Cellular Analysis (Nov. 5, 2013) ... 74a

TABLE OF AUTHORITIES

CASES

Bond v. United States, 529 U.S. 334 (2000) 27

Chapman v. United States, 365 U.S. 610 (1961) 27

Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014) 23

Ferguson v. City of Charleston, 532 U.S. 67 (2001). 27

Florida v. Jardines, 133 S. Ct. 1409 (2013) 26

In re Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011 (N.D. Cal. 2015), *appeal dismissed*, No. 15-16760 (9th Cir. Feb. 5, 2016) 29

In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) 14, 22, 34

In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304 (3d Cir. 2010) 14, 22, 23, 28

Katz v. United States, 389 U.S. 347 (1967) .....*passim*

Kyllo v. United States, 533 U.S. 27 (2001) 17, 26, 28, 30

Minnesota v. Olson, 495 U.S. 91 (1990) 27

New York v. Belton, 453 U.S. 454 (1981) 16

Riley v. California, 134 S. Ct. 2473 (2014) .....*passim*

Smith v. Maryland, 442 U.S. 735 (1979) .....*passim*

State v. Earls, 70 A.3d 630 (N.J. 2013) 24

Stoner v. California, 376 U.S. 483 (1964) 27

Tracey v. State, 152 So. 3d 504 (Fla. 2014) 24, 32

United States v. Davis, 754 F.3d 1205 (11th Cir. 2014), *rev'd en banc*, 785 F.3d 498 (11th Cir. 2015) 14, 29

United States v. Davis, 785 F.3d 498 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015) .....*passim*

United States v. Garcia, 474 F.3d 994 (7th Cir. 2007) 25

United States v. Graham, 796 F.3d 332 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016) 14

United States v. Graham, 824 F.3d 421 (4th Cir. 2016) .....*passim*

United States v. Guerrero, 768 F.3d 351 (5th Cir. 2014) 22

United States v. Jacobsen, 466 U.S. 109 (1984)..... 27

United States v. Jones, 132 S. Ct. 945 (2012) ...*passim*

United States v. Karo, 468 U.S. 705 (1984) 29

United States v. Marquez, 605 F.3d 604 (8th Cir. 2010) 25

United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) 24, 25

United States v. Miller, 425 U.S. 435 (1976) ....*passim*

United States v. Pineda-Moreno, 617 F.3d 1120 (9th Cir. 2010) 20, 25

United States v. Skinner, 690 F.3d 772 (6th Cir. 2012) 8

United States v. Knotts, 460 U.S. 276 (1983)..... 20

Zanders v. State, No. 15A01–1509-CR–1519, __ N.E.3d __, 2016 WL 4140998 (Ind. Ct. App. Aug. 4, 2016), *pet. to transfer jurisdiction to Indiana Supreme Court filed* (Sept. 6, 2016) 14, 23

CONSTITUTION & STATUTES

U.S. Const. amend. IV ..... *passim*

Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 207, 108 Stat. 4279 (1994) 33

Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848 33

Hobbs Act, 18 U.S.C. § 1951(a) 9

Stored Communications Act, 18 U.S.C. § 2703 *et seq.* ..... *passim*

18 U.S.C. § 2703(c)(1)(A) 34

18 U.S.C. § 2703(d) ..... i, 3, 22

18 U.S.C. § 924(c) 9

28 U.S.C. § 1254(1) 1

725 Ill. Comp. Stat. 168/10 24

Colo. Rev. Stat. § 16-3-303.5(2) 23

Ind. Code 35-33-5-12 24

Md. Code Ann. Crim. Proc. § 1-203.1(b) 24

Me. Rev. Stat. tit. 16, § 648 23

Minn. Stat. §§ 626A.28(3)(d), 626A.42(2) 23

Mont. Code Ann. § 46-5-110(1)(a) 23

N.H. Rev. Stat. Ann. § 644-A:2 23

Utah Code Ann. § 77-23c-102(1)(a) 23

Va. Code Ann. § 19.2-70.3(C) 24

Vt. Stat. Ann. tit. 13, § 8102(b) 23

OTHER AUTHORITIES

American Civil Liberties Union, Cell Phone Location Tracking Public Records Request (Mar. 25, 2013) 20

Andrea Meyer, *30th Anniversary of the First Commercial Cell Phone Call*, Verizon (Oct. 11, 2013) 33, 34

Arvind Thiagarajan et al., *Accurate, Low-Energy Trajectory Mapping for Mobile Devices*, 8 USENIX Conf. on Networked Syss. Design & Implementation 20 (2011) 31

AT&T, *Transparency Report* (2015) 19

Background on CTIA's Wireless Industry Survey, CTIA-The Wireless Association (2014) 33

CTIA – The Wireless Association, *Annual Wireless Industry Survey* (2014) 7, 18, 33

Daniel Solove, *Conceptualizing Privacy*, 90 Calif. L. Rev. 1087 (2002) 15

Pew Research Ctr., *Public Perceptions of Privacy and Security in the Post-Snowden Era* (Nov. 12, 2014) 32

Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 Stan. L. Rev. 119 (2002) 15

Stephen J. Blumberg & Julian V. Luke, Ctr. For Disease Control & Prevention, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, January-June 2014* (Dec. 2014) 18

T-Mobile, *Transparency Report for 2013 & 2014* (2015) 19

Will Baude, *Further Thoughts on the Precedential Status of Decisions Affirmed on Alternate Grounds*, The Volokh Conspiracy (Dec. 3, 2013, 7:27 PM), http://volokh.com/2013/12/03/thoughts-precedential-status-decisions-affirmed-alternate-grounds/ 25

PETITION FOR A WRIT OF CERTIORARI

Petitioner Timothy Carpenter respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Sixth Circuit.

OPINIONS BELOW

The opinion of the Sixth Circuit (Pet. App. 1a–32a) is reported at 819 F.3d 880. The district court opinion (Pet. App. 34a–48a) is unpublished, but is available at 2013 WL 6385838.

JURISDICTION

The Sixth Circuit issued its opinion on April 13, 2016, and denied rehearing en banc on June 29, 2016. (Pet. App. 33a). This Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS

The Fourth Amendment to the U.S. Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Stored Communications Act, 18 U.S.C. § 2703, provides in relevant part:

> **(c) Records concerning electronic communication service or remote computing service.**--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—
>
> > **(A)** obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; [or]
> >
> > **(B)** obtains a court order for such disclosure under subsection (d) of this section; * * *
>
> **(d) Requirements for court order.**--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other

> information sought, are relevant and material to an ongoing criminal investigation. * * *

STATEMENT OF THE CASE

This case presents the pressing question of whether the Fourth Amendment protects against the government's warrantless acquisition of cell phone records revealing an individual's location and movements over extended periods of time.

1. During the course of an investigation into a series of armed robberies that occurred in southeastern Michigan and northwestern Ohio in 2010 and 2011, an Assistant United States Attorney submitted to different magistrate judges three applications for orders to access more than five months of historical cell phone location records for Petitioner Timothy Carpenter and several other suspects. Pet. App. 3a, 49a–55a, 62a–68a. The applications, which were unsworn, did not seek warrants based on probable cause, but rather orders under the Stored Communications Act, 18 U.S.C. § 2703(d). Such an order may issue when the government "offers specific and articulable facts showing that there are reasonable grounds to believe that" the records sought "are relevant and material to an ongoing criminal investigation." *Id.*

The applications sought "[a]ll subscriber information, toll records and call detail records including listed and unlisted numbers dialed or otherwise transmitted to and from [the] target telephones from December 1, 2010 to present[,]" as well as "cell site information for the target telephones at call origination and at call termination

for incoming and outgoing calls[.]" Pet. App. 4a (alterations in original); *see also id.* at 52a. The applications stated that "a cooperating defendant was interviewed about his involvement in [several] armed robberies and admitted he had a role in eight different robberies that started in December of 2010 and lasted through March of 2011 at Radio Shack and T-Mobile stores in Michigan and Ohio." Pet. App. 53a. The applications further asserted that "the requested telecommunications records should yield information that is relevant and material to corroborate surveillance information and may identify potential witnesses and/or targets. The requested information will . . . provide evidence that . . . Timothy Carpenter and other known and unknown individuals are violating provisions of Title 18, United States Code, §1951." Pet. App. 54a. Rather than restricting the request to only the days on which the robberies occurred, however, the primary application at issue here, which was submitted on May 2, 2011, sought records "from December 1, 2010 to present." Pet. App. 52a. That constituted a request for 152 days of data.

Orders granting the applications were issued on May 2 and June 7, 2011. Pet. App. 56a–61a, 69a–73a. The May 2 order directed MetroPCS, Carpenter's cellular service provider, to "provide the locations of cell/site sector (physical addresses) for the target telephones at call origination and at call termination for incoming and outgoing calls" from "December 1, 2010 to present." Pet. App. 59a–60a. MetroPCS complied, providing 186 pages of

Carpenter's cell phone records to the government.[1] Those records show each of Carpenter's incoming and outgoing calls over the course of 127 days,[2] along with the cell tower ("cell site") and directional sector of the tower that Carpenter's phone connected to at the start and end of most of the calls.[3] Pet. App. 5a–7a.

A separate order, issued on June 7, 2011, directed Sprint to produce cell site location information for Carpenter's phone while it was "roaming on Sprint's cellular tower network" from March 1 to March 7, 2011. Pet. App. 72a. "Metro PCS does not have coverage in the Warren, Ohio area," where one of the charged robberies took place, and

---

[1] A sample page from Carpenter's records was entered into evidence at trial. Defendant's Trial Ex. 3. The full records were provided by the government to the defense in pre-trial discovery and were discussed by a prosecution's witness at trial, Trial Tr. 46, Dec. 13, 2013, ECF No. 332, but were not made part of the record before the district court. They were filed as an appendix to the Amicus Brief of the American Civil Liberties Union, et al., at the Sixth Circuit. *See* Doc. No. 33-1 The parties stipulated at trial that the cell site location records from "Metro PCS and Sprint utilized by [government witness] FBI Special Agent Christopher Hess to formulate his analysis and opinion are authentic and accurate business records of these companies." Gov't Trial Ex. 58; Trial Tr. 47, Dec. 13, 2013, ECF No. 332.

[2] Although the government's application and resulting court order sought 152 days of records (December 1, 2010 through May 2, 2011), MetroPCS produced 127 days of records (December 1, 2010 through April 6, 2011).

[3] Cell sites, which are the transmitting towers through which cell phones communicate with the telephone network, consist of antennas facing different directions that cover distinct wedge-shaped "sectors."

has a "roaming agreement . . . with Sprint, which does cover that area." Trial Tr. 59, Dec. 13, 2013. ECF No. 332.[4] Therefore, Sprint, not MetroPCS, possessed Carpenter's cell site location information for calls made and received while he was in Ohio. Sprint produced two pages of call detail records with cell site location information for March 3 and 4, 2011.

MetroPCS and Sprint also produced lists of their cell sites in southern Michigan and northwestern Ohio, respectively, providing the longitude, latitude, and physical address of each cell site, along with the directional orientation of each sector antenna. *See id.* at 74. By cross-referencing the information in Carpenter's call detail records with these cell-site lists, the government could identify the area in which Carpenter's phone was located and could thereby deduce Carpenter's location and movements at multiple points each day.

2. The precision of a cell phone user's location reflected in cell site location information ("CSLI") records depends on the size of the cell site sectors in the area. Most cell sites consist of multiple directional antennas that divide the cell site into "sectors." Pet. App. 5a. The coverage area of cell site sectors is smaller in areas with greater density of cell towers, with urban areas having the greatest density and thus the smallest coverage areas. *Id.*; *see also* Pet. App. 88a (Gov't Trial Ex. 57, at 13) (providing maps of MetroPCS and Sprint cell sites).

---

[4] As explained at trial, "[i]n a roaming situation, if [a service provider] doesn't have coverage in a particular area of the country, they would have an agreement with another company to be able to utilize their infrastructure." *Id.* at 39–40.

The density of cell sites continues to increase as data usage from smartphones grows. Because each cell site can carry only a fixed volume of data required for text messages, emails, web browsing, streaming video, and other uses, as smartphone data usage increases carriers must erect additional cell sites, each covering smaller geographic areas. *See* CTIA - The Wireless Association, *Annual Wireless Industry Survey* (2016)[5] (showing that the number of cell sites in the United States increased from 183,689 to 307,626 from 2005 to 2015); *id.* (annual wireless data usage increased from 388 billion megabytes to 9.65 trillion megabytes between 2010 and 2015). This means that in urban and dense suburban areas like Detroit, many sectors cover small geographic areas and therefore can provide relatively precise information about the location of a phone. Pet. App. 5a.

Although in this case MetroPCS provided only information identifying Carpenter's cell site and sector at the start and end of his calls, service providers increasingly retain more granular historical location data, including for text messages and data connections. *United States v. Davis*, 785 F.3d 498, 542 (11th Cir. 2015) (en banc) (Martin, J., dissenting). Location precision is also increasing as service providers deploy millions of "small cells," "which cover a very specific area, such as one floor of a building, the waiting room of an office, or a single home." *United States v. Graham*, 824 F.3d 421, 448 (4th Cir. 2016) (en banc) (Wynn, J., dissenting in

---

[5] *Available at* http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey.

part and concurring in the judgment) (citation omitted).

3. Before trial, Carpenter joined his codefendant's motion to suppress the CSLI records on the basis that their acquisition pursuant to the "'reasonable grounds standard' in the Stored Communications Act . . . is unconstitutional." Pet. App. 36a; *see also id.* at 4a. Relying on *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012), a case holding that no warrant is required for short-term real-time tracking of a suspect's cell phone, the district court denied the motion on the basis that acquisition of the cell-site records was not a Fourth Amendment search. Pet. App. 38a–39a.

At trial, the government introduced information about Carpenter's CSLI records and relied on them to establish Carpenter's location on the days of the charged robberies. FBI Special Agent Christopher Hess testified that Carpenter's CSLI records placed him near the sites of four of the robberies. Pet. App. 5a–6a. Hess also produced maps showing the location of Carpenter's phone relative to the locations of the robberies, which the government introduced into evidence. Pet. App. 6a; *Id.* at 86a–89a (Gov't Trial Ex. 57). The government relied on the records to show Carpenter's proximity to "the robberies around the time the robberies happened." Pet. App. 6a. The prosecutor argued to the jury, for example, that Mr. Carpenter was "right where the first robbery was at the exact time of the robbery, the exact sector," Trial Tr. 56, Dec. 16, 2013, ECF No. 333, and that he was "right in the right sector before the Radio Shack in Highland Park," *id. See also* Trial

Tr. 49 62, Dec. 13, 2013, ECF No. 332 (testimony of Special Agent Hess).

The jury convicted Carpenter of six robberies in violation of the Hobbs Act, 18 U.S.C. § 1951(a), and five separate violations of 18 U.S.C. § 924(c) for using or carrying a firearm in connection with a federal crime of violence and aiding and abetting. All but the first of the § 924(c) convictions carried mandatory consecutive minimum sentences of 25 years each. As a result, the court sentenced Carpenter to nearly 116 years' imprisonment (1,395 months).

5. On appeal, a divided three-judge panel of the Sixth Circuit held that no search occurred under the Fourth Amendment because Carpenter had no reasonable expectation of privacy in cell phone location records held by his service provider. Pet. App. 17a. Writing for the majority, Judge Kethledge concluded that people do not have a reasonable expectation of privacy in CSLI because it is a business record of the service provider that reveals routing information rather than the contents of communications. Pet. App. 10a–11a. Judge Kethledge relied in part on this Court's 1979 decision in *Smith v. Maryland*, 442 U.S. 735 (1979), reasoning that like the dialed phone numbers conveyed to the phone company in *Smith*, people knowingly expose their location information to their service provider and therefore lack an expectation of privacy in it. Pet. App. 11a–12a.

Judge Stranch disagreed. Concurring in the judgment only, she explained that "the sheer quantity of sensitive information procured without a warrant in this case raises Fourth Amendment

concerns of the type the Supreme Court . . . acknowledged in *United States v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring)." Pet. App. 24a. "I do not think that treating the CSLI obtained as a 'business record' and applying that test addresses our circuit's stated concern regarding long-term, comprehensive tracking of an individual's location without a warrant." *Id.* at 29a. Judge Stranch concluded, however, that suppression was not warranted under the good-faith exception to the exclusionary rule, a question that the majority did not address. *Id.* at 29a-31a. On that alternative basis, she concurred in the judgment.

REASONS FOR GRANTING THE WRIT

I. THIS CASE PRESENTS AN IMPORTANT AND RECURRING QUESTION ON THE SCOPE OF CONSTITUTIONAL PRIVACY RIGHTS IN THE DIGITAL AGE.

A. The Lower Courts Have Expressly and Repeatedly Sought This Court's Guidance in Addressing the Question Presented.

The question at the center of this case—whether there is a reasonable expectation of privacy under the Fourth Amendment in a person's cell site location information held by their cellular service provider—requires definitive resolution by this Court. Numerous lower court judges addressing the issue have explained that they feel bound by this Court's third-party-doctrine cases from the 1970s, but that they are discomfited by the result they believe those cases require them to reach. Only this Court can provide the guidance they seek about

whether and how a doctrine developed long before the digital age applies to the voluminous and sensitive digital records at issue here. More specifically, only this Court can determine whether *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), render the Fourth Amendment irrelevant when the government seeks detailed records from a cell phone provider cataloging the location and movements of a cell phone user over many months.

In *Smith*, this Court ruled that the short-term use of a pen register to capture the telephone numbers a person dials is not a search under the Fourth Amendment. 442 U.S. at 742. The Court relied heavily on the fact that when dialing a phone number, the caller "voluntarily convey[s] numerical information to the telephone company." *Id.* at 744. The Court also assessed the degree of invasiveness of the surveillance to determine whether the user had a reasonable expectation of privacy. The Court noted the "pen register's limited capabilities," *id.* at 742, explaining that "a law enforcement official could not even determine from the use of a pen register whether a communication existed." *Id.* at 741 (citation omitted). Similarly, in *Miller*, the Court concluded that bank customers do not have any Fourth Amendment interest in their bank records because all the information in those records has been voluntarily conveyed to the bank. 425 U.S. 435, 440 42 (1976). The principle sometimes discerned from these cases, that certain records or information shared with third parties deserve no Fourth Amendment protection, is known as the "third-party doctrine."

Lacking further guidance from this Court, lower courts have been struggling to apply the pre-digital holdings in *Smith* and *Miller* to newer forms of pervasive digital data.

In *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (en banc), *cert. denied*, 136 S. Ct. 479 (2015), for example, a majority of the en banc Eleventh Circuit held that this Court's decisions in *Smith* and *Miller* require the conclusion that there is no Fourth Amendment protection for CSLI records. But while the Eleventh Circuit believed it "remains bound by *Smith* and *Miller*," 785 F.3d at 514, two separate concurrences called on this Court to clarify the scope of those decisions, evincing discomfort with their application to the records at issue. As Judge Rosenbaum wrote:

> In our time, unless a person is willing to live "off the grid," it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life. And the thought that the government should be able to access such information without the basic protection that a warrant offers is nothing less than chilling. . . . Since we are not the Supreme Court and the third-party doctrine continues to exist and to be good law at this time, though, we must apply the third-party doctrine where appropriate.

Id. at 525 (Rosenbaum, J., concurring); *see also id.* at 519, 521 (William Pryor, J., concurring) ("[W]e must leave to the Supreme Court the task of developing

exceptions to the rules it has required us to apply. . . . As judges of an inferior court, we have no business in anticipating future decisions of the Supreme Court. If the third-party doctrine results in an unacceptable 'slippery slope,' the Supreme Court can tell us as much. That is, if 'the Supreme Court has given reasons to doubt the rule's breadth,' it alone must decide the exceptions to its rule." (citations omitted)).

Likewise, the en banc majority of the Fourth Circuit wrote that "[t]he Supreme Court may in the future limit, or even eliminate, the third-party doctrine. . . . But without a change in controlling law, we cannot conclude that the Government violated the Fourth Amendment in this case." *United States v. Graham*, 824 F.3d 421, 425 (4th Cir. 2016) (en banc). And in this case, Judge Stranch discussed her "concern[] about the applicability of a test that appears to admit to no limitation on the quantity of records or the length of time for which such records may be compelled," concluding that there is a "need to develop a new test to determine when a warrant may be necessary under these or comparable circumstances." Pet. App. 29a (Stranch, J., concurring).

All told, the five courts of appeals to consider the Fourth Amendment status of historical CSLI have generated 18 separate majority, concurring, and dissenting opinions, highlighting the need for this Court to act. *See* Pet. App. 1a (majority opinion); *id.* at 24a (Stranch, J., concurring); *United States v. Graham*, 824 F.3d 421, 424 (4th Cir. 2016) (en banc) (majority opinion); *id.* at 438 (Wilkinson, J., concurring); *id.* at 441 (Wynn, J., dissenting in part

and concurring in the judgment); *United States v. Graham*, 796 F.3d 332, 338 (4th Cir. 2015) (majority opinion), *vacated, reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015); *id.* at 377 (Thacker, J., concurring); *id.* at 378 (Motz, J., dissenting in part and concurring in the judgment); *United States v. Davis*, 785 F.3d 498, 500 (11th Cir. 2015) (en banc) (majority opinion); *id.* at 519 (William Pryor, J., concurring); *id.* at 521 (Jordan, J., concurring); *id.* at 524 (Rosenbaum, J., concurring); *id.* at 533 (Martin, J., dissenting); *United States v. Davis*, 754 F.3d 1205, 1208 (11th Cir. 2014) (unanimous), *vacated, reh'g en banc granted*, 573 F. App'x 925 (11th Cir. 2014); *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 602 (5th Cir. 2013) [*"Fifth Circuit CSLI Opinion"*] (majority opinion); *id.* at 615 (Dennis, J., dissenting); *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 305 (3d Cir. 2010) [*"Third Circuit CSLI Opinion"*] (majority opinion); *id.* at 319 (Tashima, J., concurring).

As reflected in these 18 opinions attempting to grapple with the same basic issue, lower courts are divided over how to apply the third-party doctrine to CSLI records. *Compare Graham*, 824 F.3d at 424–25 (no expectation of privacy in CSLI under *Smith*), *Davis*, 785 F.3d at 511–13 (same), *and Fifth Circuit CSLI Opinion*, 724 F.3d at 612–13 (same), *with Third Circuit CSLI Opinion*, 620 F.3d at 317 (distinguishing *Smith* and holding that cell phone users may retain a reasonable expectation of privacy in CSLI); *Zanders v. State*, No. 15A01–1509–CR–1519, __ N.E.3d __, 2016 WL 4140998, at *8–10 (Ind. Ct. App. Aug. 4, 2016) (distinguishing *Smith* and *Miller* and holding that "the third-party doctrine

does not dictate the outcome of this case"), *pet. to transfer jurisdiction to Indiana Supreme Court filed* (Sept. 6, 2016).

This struggle to define the scope of Fourth Amendment protection for newer forms of sensitive digital data reflects, at least in part, scholarly criticism of the expansive application of the third-party doctrine beyond the kinds of records at issue in *Smith* and *Miller*. *See, e.g.*, Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 Stan. L. Rev. 119 (2002); Daniel J. Solove, *Conceptualizing Privacy*, 90 Calif. L. Rev. 1087, 1151–52 (2002). These scholars have joined the lower courts in calling on this Court to ensure that the Fourth Amendment keeps pace with the rapid advance of technology.

In sum, there is a substantial question of how the protections of the Fourth Amendment should apply to sensitive and private data in the hands of trusted third parties. As Justice Sotomayor noted in *United States v. Jones*,

> it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.

132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

It is not necessary in this case to reassess the continued validity of the third-party doctrine in every possible context. But it is critically important to clarify the scope of analog-age precedents to digital surveillance techniques. Without guidance from this Court, a cell phone user "cannot know the scope of his constitutional protection, nor can a policeman know the scope of his authority." *New York v. Belton*, 453 U.S. 454, 459–60 (1981). As law enforcement seeks ever greater quantities of location data and other sensitive digital records, the need for this Court to speak grows daily more urgent.

B. This Court's Recent Decisions Have Properly Recognized a Need to Reexamine Traditional Understandings of Privacy in the Digital Age.

Twice in recent terms this Court has confronted crucial questions regarding the application of the Fourth Amendment in the digital age. *See Riley v. California*, 134 S. Ct. 2473 (2014) (warrant required for search of cell phone seized incident to lawful arrest); *United States v. Jones*, 132 S. Ct. 945 (2012) (tracking car with GPS device is a Fourth Amendment search). This case presents an important next step in the ongoing effort to reconcile enduring Fourth Amendment principles with the reality of a new digital world.

In *United States v. Jones*, this Court addressed the pervasive location monitoring made possible by GPS tracking technology surreptitiously and warrantlessly attached to a vehicle. All members of the Court agreed that attaching a GPS device to a vehicle and tracking its movements constitutes a

search under the Fourth Amendment. In so holding, the Court made clear that the government's use of novel digital surveillance technologies not in existence at the framing of the Fourth Amendment does not escape the Fourth Amendment's reach. 132 S. Ct. at 950–51 ("[W]e must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001))); *id.* at 963–64 (Alito, J., concurring in the judgment) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.").

In *Riley v. California*, the Court addressed Americans' privacy rights in the contents of their cell phones, unanimously holding that warrantless search of the contents of a cell phone incident to a lawful arrest violates the Fourth Amendment. In so doing, the Court rejected the government's inapt analogy to other physical objects that have historically been subject to warrantless search incident to an arrest. 134 S. Ct. at 2489 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person.").

Monitoring an individual's location and movements over an extended period of time by collecting and analyzing cell phone records can and frequently will expose extraordinarily sensitive details of a person's life including, potentially, "a wealth of detail about . . . familial, political, professional, religious, and sexual associations."

Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring). Without disputing that premise, the court of appeals nonetheless held that this voluminous documentation of a person's movements in public *and* private spaces is unprotected by the Fourth Amendment by analogizing to the kinds of limited analog data at issue in *Smith* and *Miller*. Pet. App. 11a–14a. As this Court recently cautioned, however, unexamined reliance on "pre-digital analogue[s]" risks causing "a significant diminution of privacy." *Riley*, 134 S.Ct. at 2493. Accordingly, "any extension of . . . reasoning [from decisions concerning analog searches] to digital data has to rest on its own bottom." *Id.* at 2489. Only this Court can make that ultimate constitutional judgment.

C. The Volume and Frequency of Warrantless Law Enforcement Requests for CSLI Highlights the Importance of the Question Presented.

"[M]ore than 90% of American adults . . . own a cell phone." *Riley*, 134 S. Ct. at 2490. As of December 2015, there were more than 377 million wireless subscriber accounts in the United States.[6] Forty-four percent of U.S. households have *only* cell phones.[7] When "nearly three-quarters of smart phone

---

[6] CTIA The Wireless Association, *Annual Wireless Industry Survey* (2016), http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey.

[7] Stephen J. Blumberg & Julian V. Luke, Ctr. For Disease Control & Prevention, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, January–June 2014* 1 (Dec. 2014), http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201412.pdf.

users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower," *Riley*, 134 S. Ct. at 2490, the privacy implications of warrantless law enforcement access to cell phone location data are difficult to overstate.

This is not an isolated or occasional concern. Law enforcement is requesting staggering volumes of CSLI from service providers. From July 2015 to June 2016, for example, AT&T received 75,302 requests for cell phone location information.[8] Verizon received approximately 18,935 requests for cell phone location data in just the first half of 2016.[9]

The government often obtains large volumes of CSLI pursuant to such requests. In this case the government requested five months' and obtained nearly four months' (127 days') worth of Carpenter's location data comprising thousands of location data points. A request for months of data is no aberration: according to T-Mobile, which now owns Carpenter's service provider, MetroPCS, the average law enforcement request "asks for approximately fifty-five days of records."[10] Other recent and pending cases involve comparable or even greater quantities

---

[8] AT&T, *Transparency Report*, at 4 (2016), http://about.att.com/content/dam/csr/Transparency%20Reports/ATT TransparencyReport_July2016.pdf .

[9] Verizon, *Transparency Report 1H 2016*, at 5 (2016), https://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2016/07/Transparency-Report US-1H-2016.pdf.

[10] T-Mobile, *Transparency Report for 2013 & 2014*, at 5 (2015), http://newsroom.t-mobile.com/content/1020/files/NewTransparencyReport.pdf.

of sensitive location information obtained without a warrant. In one case, the government obtained 221 days (more than seven months) of cell site location information, revealing 29,659 location points for one defendant. *See Graham*, 824 F.3d at 446–47 (Wynn, J., dissenting in part and concurring in the judgment).

In *Jones*, Justice Alito recognized that of the "many new devices that permit the monitoring of a person's movements," cell phones are "[p]erhaps most significant." 132 S. Ct. at 963 (Alito, J., concurring in the judgment). Yet most law enforcement agencies are obtaining these large quantities of historical CSLI without a probable cause warrant. *See* American Civil Liberties Union, Cell Phone Location Tracking Public Records Request (Mar. 25, 2013)[11] (responses to public records requests sent to roughly 250 local law enforcement agencies show that "few agencies consistently obtain warrants" for CSLI). The volume of warrantless requests for CSLI and the ubiquity of cell phones make the question presented one of compelling national importance.

Judge Kozinski has summarized the situation well. In an opinion written six years ago, he began by noting that this Court's decision in *United States v. Knotts*, 460 U.S. 276, 283-84 (1983), expressly left open the question whether "'twenty-four hour surveillance of any citizen of this country' by means of 'dragnet-type law enforcement practices' violates the Fourth Amendment's guarantee of personal privacy." *United States v. Pineda-Moreno*, 617 F.3d

---

[11] https://www.aclu.org/cases/cell-phone-location-tracking-public-records-request.

1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing *en banc*). He then cogently observed, "[w]hen requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that 'such dragnet-type law enforcement practices' are already in use." *Id.* What was true six years ago is even more true today. This Court's intervention is needed now to ensure that the Fourth Amendment does not become a dead letter as police accelerate their warrantless access to rich troves of sensitive personal location data.

II. FEDERAL COURTS OF APPEALS AND STATE HIGH COURTS ARE DIVIDED.

The Sixth Circuit's decision in this case widens the conflict over whether, or in what circumstances, sensitive cell phone location data held in trust by a service provider is protected by a warrant requirement.

A. The Circuits Are Split Over Whether the Third-Party Doctrine Eliminates People's Reasonable Expectation of Privacy in Their Historical CSLI.

The Sixth Circuit joins the Fourth, Fifth, and Eleventh Circuits in holding that there is no reasonable expectation of privacy in historical cell site location information under the Fourth Amendment, and therefore that no warrant is required. In the first of these decisions, *In re Application of the U.S. for Historical Cell Site Data*,

724 F.3d 600 (5th Cir. 2013), a magistrate judge rejected a government application for an order pursuant to the Stored Communications Act, 18 U.S.C. § 2703(d), seeking historical CSLI, holding that a warrant is required under the Fourth Amendment. On appeal, a divided panel of the Fifth Circuit held that any expectation of privacy in CSLI is vitiated by the cell service provider's creation and possession of the records. 724 F.3d at 613. The court rejected the argument that cell phone users retain an expectation of privacy in the data because they do not voluntarily convey their location information to the service provider. *Id.* at 613–14; *see also United States v. Guerrero*, 768 F.3d 351, 358–59 (5th Cir. 2014) (applying *In re Application* in the context of a suppression motion). The Fourth and Eleventh Circuits have subsequently agreed with this position. *Graham*, 824 F.3d at 424–25; *Davis*, 785 F.3d at 511–13.

The Third Circuit takes the contrary position. *See Fifth Circuit CSLI Opinion*, 724 F.3d at 616 (Dennis, J., dissenting) (recognizing split between Third and Fifth Circuits). In a decision issued more than a year before this Court's opinion in *Jones*, the Third Circuit held that magistrate judges have discretion to require a warrant for historical CSLI if they determine that the location information sought will implicate the suspect's Fourth Amendment privacy rights by showing, for example, when a person is inside a constitutionally protected space. *Third Circuit CSLI Opinion*, 620 F.3d at 319. In reaching that conclusion, the court rejected the argument that a cell phone user's expectation of privacy is eliminated by the service provider's ability to access that information:

> A cell phone customer has not "voluntarily" shared his location information with a cellular provider in any meaningful way. . . . [I]t is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information. Therefore, "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all."

Id. at 317–18 (last alteration in original). Therefore, the court held, the third-party doctrine does not apply to historical CSLI records. *Id.*

This split in the circuits is accentuated by the growing number of states that require a warrant for historical CSLI by statute or pursuant to judicial opinion. *See Zanders v. State*, No. 15A01–1509–CR–1519, __ N.E.3d __, 2016 WL 4140998 (Ind. Ct. App. Aug. 4, 2016); *Commonwealth v. Augustine*, 4 N.E.3d 846 (Mass. 2014); Colo. Rev. Stat. § 16-3-303.5(2); Me. Rev. Stat. tit. 16, § 648; Minn. Stat. §§ 626A.28(3)(d), 626A.42(2); Mont. Code Ann. § 46-5-110(1)(a); Utah Code Ann. § 77-23c-102(1)(a); N.H. Rev. Stat. Ann. § 644-A:2; 2016 Vt. Laws No. 169 (S. 155) (to be codified at Vt. Stat. Ann. tit. 13, § 8102(b)). Additional states require a warrant for real-time cell phone location data. *See, e.g., Tracey v.*

State, 152 So. 3d 504 (Fla. 2014); *State v. Earls*, 70 A.3d 630 (N.J. 2013); 725 Ill. Comp. Stat. 168/10; Ind. Code 35-33-5-12; Md. Code Ann. Crim. Proc. § 1-203.1(b); Va. Code Ann. § 19.2-70.3(C). Requiring a warrant for CSLI would harmonize the protections available to people throughout the United States.

B. The Circuits Are Split Over Whether There is a Reasonable Expectation of Privacy in Longer-Term Location Information Collected by Electronic Means.

In *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *aff'd on other grounds sub nom. Jones*, 132 S. Ct. 945, the D.C. Circuit held that using a GPS device to surreptitiously track a car over the course of 28 days violates reasonable expectations of privacy and is therefore a Fourth Amendment search. *Id.* at 563. The court explained that "[p]rolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation." *Id.* at 562. Therefore, people have a reasonable expectation of privacy in the intimate and private information revealed by "prolonged GPS monitoring." *Id.* at 563.

Although this Court affirmed on other grounds, relying on a trespass-based rationale, the D.C. Circuit's approach under the *Katz* reasonable-expectation-of-privacy test remains controlling law in

that circuit.[12] And that holding does not depend on the nature of the tracking technology at issue: prolonged electronic surveillance of the location of a person's cell phone is at least as invasive as prolonged electronic surveillance of the location of her car. *See Jones*, 132 S. Ct. at 963 (Alito, J., concurring in the judgment) (explaining that law enforcement access to cell phone location information is "[p]erhaps most significant" of the "many new devices that permit the monitoring of a person's movements.").

The Sixth Circuit rejected this reasoning when it held that the information contained in CSLI records is categorically unprotected by the Fourth Amendment, regardless of what it reveals and over what period of time. Pet. App. 13a–14a. In doing so, the court of appeals widened the circuit split over whether people have a reasonable expectation of privacy in their longer-term location information—a split that existed prior to *Jones* and continues today. *Compare Maynard*, 615 F.3d at 563 (prolonged electronic location tracking is a search under the Fourth Amendment), *with Pineda-Moreno*, 591 F.3d at 1216–1217 (prolonged electronic location tracking is not a search under the Fourth Amendment), *United States v. Garcia*, 474 F.3d 994, 996–99 (7th Cir. 2007) (same), *and United States v. Marquez*, 605 F.3d 604, 609 (8th Cir. 2010) ("A person traveling via automobile on public streets has no reasonable

---

[12] *See* Will Baude, *Further Thoughts on the Precedential Status of Decisions Affirmed on Alternate Grounds*, The Volokh Conspiracy (Dec. 3, 2013, 7:27 PM), http://volokh.com/2013/12/03/thoughts-precedential-status-decisions-affirmed-alternate-grounds/.

expectation of privacy in his movements from one locale to another.").

III. THE SIXTH CIRCUIT ERRED IN HOLDING THAT THE CONDUCT HERE WAS NOT A SEARCH.

A. The Sixth Circuit Erred in Holding That There Is No Reasonable Expectation of Privacy in Historical CSLI.

The Sixth Circuit majority held that the mere fact that the government obtained the CSLI records from Petitioner's service provider, rather than from Petitioner himself, dooms his Fourth Amendment claim in light of *United States v. Miller* and *Smith v. Maryland*. Neither *Miller* nor *Smith* compels that conclusion and this Court should reject that understanding of its prior precedent. The mere fact that another person or entity has access to or control over private records does not in itself—and without regard to any other circumstance—destroy an otherwise reasonable expectation of privacy. Though third-party access to records may be one factor weighing on the *Katz* reasonable-expectation-of-privacy analysis, the third-party doctrine elucidated in *Miller* and *Smith* is not and never has been an on-off switch. *See Florida v. Jardines*, 133 S. Ct. 1409, 1418–19 (2013) (Kagan, J., concurring) (expectation of privacy in odors detectable by a police dog that emanate from a home); *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) (information about location and movement in public, even though exposed to public view); *Kyllo*, 533 U.S. 27 (thermal signatures emanating from a home); *Ferguson v. City*

of Charleston, 532 U.S. 67, 78 (2001) ("The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."); *Bond v. United States*, 529 U.S. 334, 336 (2000) (bag exposed to the public on luggage rack of bus); *Minnesota v. Olson*, 495 U.S. 91, 98–99 (1990) ("an overnight guest has a legitimate expectation of privacy in his host's home" even though his possessions may be disturbed by "his host and those his host allows inside"); *United States v. Jacobsen*, 466 U.S. 109, 115 (1984) (reasonable expectation of privacy in letters and sealed packages entrusted to private freight carrier); *Katz v. United States*, 389 U.S. 347 (1967) (reasonable expectation of privacy in contents of phone call even though call is conducted over private companies' networks); *Stoner v. California*, 376 U.S. 483, 487–90 (1964) (implicit consent to janitorial personnel to enter motel room does not amount to consent for police to search room); *Chapman v. United States*, 365 U.S. 610, 616 17 (1961) (search of a house invaded tenant's Fourth Amendment rights even though landlord had authority to enter house for some purposes).

The Sixth Circuit erred in treating the fact of third party access to the records as dispositive. Pet. App. 14a. This Court should make clear that the reasonable-expectation-of-privacy test relies on a totality-of-the-circumstances analysis. Avoiding mechanical applications of holdings from the analog age is of paramount importance when dealing with highly sensitive and voluminous digitized records. *See Riley*, 134 S. Ct. at 2489. It is virtually impossible to participate fully in modern life without

leaving a trail of digital breadcrumbs that create a pervasive record of the most sensitive aspects of our lives. Ensuring that technological advances do not "erode the privacy guaranteed by the Fourth Amendment," *Kyllo*, 533 U.S. at 34, requires nuanced applications of analog-age precedents.

This is not to say that proper resolution of this case requires wholesale rejection of *Smith* and *Miller*'s holdings. Even on the plain terms of those decisions, Petitioner retains a reasonable expectation of privacy in his CSLI.

To assess an individual's expectation of privacy in records held by a third party this Court has looked to, among other factors, whether the records were "voluntarily conveyed" to that entity, *Miller*, 425 U.S. at 442; *Smith*, 442 U.S. at 744, and what privacy interest a person has in the information the records reveal, *Miller*, 425 U.S. at 442; *Smith*, 442 U.S. at 741–42. Unlike the dialed phone numbers and limited bank records at issue in *Smith* and *Miller*, "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way." *Third Circuit CSLI Opinion*, 620 F.3d at 317. Location information is not entered by the user into the phone, nor otherwise affirmatively transmitted to the service provider. This is doubly true when a person receives a call, thereby taking *no* action that would knowingly or voluntarily reveal location. *Id.* at 317–18. It is also particularly clearly the case when that person's cell phone is roaming on another carrier's network, as was Carpenter's here, because "[t]ypically, a cell phone user does not know when her phone is roaming onto another provider's

network, much less the name of the other provider on whose network her phone is roaming." *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011, 1028–29 (N.D. Cal. 2015), *appeal dismissed*, No. 15-16760 (9th Cir. Feb. 5, 2016). "As a result, cell phone users, unlike a bank depositor or telephone dialer, will often not know the identity of the third party to which they are supposedly conveying information." *Id.* at 1029.

Moreover, the documentation of a person's movements, locations, and activities over the course of time contained in CSLI records is exceedingly sensitive and private in ways that were not at issue in *Smith* or *Miller*. This is so for at least two reasons. First, because people carry their phones with them virtually everywhere they go, including inside their homes and other constitutionally protected spaces, cell phone location records can reveal information about presence, location, and activity in those spaces. *See United States v. Davis*, 754 F.3d 1205, 1215-16 (11th Cir. 2014) (Sentelle, J.), *rev'd en banc*, 785 F.3d 498 (11th Cir. 2015). In *United States v. Karo*, 468 U.S. 705 (1984), this Court held that location tracking implicates Fourth Amendment privacy interests when it may reveal information about individuals in areas where they have reasonable expectations of privacy. The Court explained that using an electronic device—there, a beeper—to infer facts about "location[s] not open to visual surveillance," like whether "a particular article is actually located at a particular time in the private residence," or to later confirm that the article remains on the premises, was just as unreasonable as physically searching the location without a warrant. *Id.* at 714–16. Such location tracking "falls

within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance" from a public place. *Id.* at 707; *see also Kyllo*, 533 U.S. at 36 (use of thermal imaging device to learn information about interior of home constitutes a search).

Second, CSLI reveals a great sum of sensitive and private information about a person's movements and activities in public and private spaces that, at least over the longer term, violates expectations of privacy. In *Jones*, although the majority opinion relied on a trespass-based rationale to determine that a search had taken place, 132 S. Ct. at 949, it specified that "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* [reasonable-expectation-of-privacy] analysis." *Id.* at 953. Five Justices conducted a *Katz* analysis, and concluded that at least longer-term location tracking violates reasonable expectations of privacy. *Id.* at 960, 964 (Alito, J., concurring in the judgment); *id.* at 955 (Sotomayor, J., concurring).

This conclusion did not depend on the particular type of tracking technology at issue in *Jones*. As Justice Sotomayor explained, electronic location tracking implicates the Fourth Amendment because it "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* at 955. This Court subsequently amplified that point when it explained that cell phone location data raises particularly acute privacy concerns because it "can reconstruct someone's specific movements down to

the minute, not only around town but also within a particular building." *Riley*, 134 S. Ct. at 2490 (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)).

The records obtained by the government in this case implicate both the expectation of privacy in private spaces and the expectation of privacy in longer-term location information. They allow the government to know or infer when a person slept at home and when he didn't. *Davis*, 785 F.3d at 540–41 (Martin, J., dissenting). They show a person's movements around town, nearly down to the minute.[13] *Id.* They even allow the government to learn who a person associated with and when. *See, e.g.*, Pet. App. 81a–82a (concluding that co-defendants were at the same location based on their CSLI records); Trial Tr. 107, Dec. 16, 2013, ECF No. 333 (same).

It is not surprising, therefore, that polling data shows that more than 80 percent of people consider

---

[13] Even knowing only periodic information about which cell sites a phone connects to over time can be used to interpolate the path the phone user traveled, thus revealing information beyond just where the phone was located at discrete points. *See, e.g.*, Arvind Thiagarajan et al., *Accurate, Low-Energy Trajectory Mapping for Mobile Devices*, 8 USENIX Conf. on Networked Syss. Design & Implementation 20 (2011), https://www.usenix.org/legacy/events/nsdi11/tech/full_papers/Thiagarajan.pdf?CFID=23055068 5&CFTOKEN=76524860 (describing one algorithm for accurate trajectory interpolation using cell site information). Law enforcement routinely uses cell site data for this purpose; in this case, the government presented testimony explaining that cell site data points revealed Carpenter's trajectories placing him at the businesses in question at the relevant times. *See* Trial Tr. 55, 57, 62, Dec. 13, 2013, ECF No. 332.

"[d]etails of [their] physical location over time" to be "sensitive"—evincing greater concern over this information than over the contents of their text messages, a list of websites they have visited, or their relationship history.[14] Historical CSLI enables the government to "monitor and track our cell phones, and thus ourselves, with minimal expenditure of funds and manpower, [which] is just the type of gradual and silent encroachment into the very details of our lives that we as a society must be vigilant to prevent." *Tracey*, 152 So. 3d at 522 (internal quotation marks omitted).

B. The Sixth Circuit Erred In Deferring to Congress's 30-Year-Old Legislative Scheme.

In concluding that the Fourth Amendment does not protect people's cell site location records from warrantless search, the Sixth Circuit majority explained that "Congress has specifically legislated on the question before us today, and in doing so has struck the balance reflected in the Stored Communications Act." Pet. App. 15a. Thus, "society itself—in the form of its elected representatives in Congress—has already struck a balance that it thinks reasonable." *Id.* at 16a. Therefore, the majority wrote, "[t]here is considerable irony in [a] request" to "declare that balance unconstitutional." *Id.* at 15a.

---

[14] Pew Research Ctr., *Public Perceptions of Privacy and Security in the Post-Snowden Era*, 32, 34 (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

The supposed balance to which the majority refers is decades old, and is a relic of legislation passed before the proliferation of cell phones and the availability of large volumes of increasingly precise cell site location information. When Congress passed the Stored Communications Act in 1986,[15] there were a mere 1,000 cell sites in the United States[16] (compared to more than 300,000 today)[17] and less than one half of one percent of Americans had a cell phone.[18] Congress gave no indication that it even considered the existence of historical CSLI, not to mention the possibility that law enforcement might want to access it. When Congress amended the Stored Communications Act in 1994,[19] cellular networks were still fragmented and rudimentary, with less than 18,000 cell sites across the country.[20] Congress simply did not contemplate the contemporary ubiquity of cell phones and the volume

---

[15] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848.

[16] Andrea Meyer, *30th Anniversary of the First Commercial Cell Phone Call*, Verizon (Oct. 11, 2013), https://www.verizonwireless.com/news/article/2013/10/30th-anniversary-cell-phone.html and https://www.slideshare.net/slideshow/embed_code/27105077?rel=0

[17] CTIA – The Wireless Association, *Annual Wireless Industry Survey*.

[18] Meyer, *30th Anniversary of the First Commercial Cell Phone Call*.

[19] Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 207, 108 Stat. 4279 (1994).

[20] *Background on CTIA's Wireless Industry Survey* 2, CTIA-The Wireless Association (2014), http://www.ctia.org/docs/default-source/Facts-Stats/ctia_survey_ye_2013_graphics-final.pdf.

and precision of CSLI when crafting the SCA. Courts should not give undue weight to this outdated legislative scheme in evaluating people's reasonable expectation of privacy under the Fourth Amendment.

Moreover, in concluding that acquisition of historical CSLI is a Fourth Amendment search, a court need not hold the Stored Communications Act unconstitutional. The SCA contains a mechanism for law enforcement to obtain a warrant for CSLI. *See* 18 U.S.C. § 2703(c)(1)(A). "Section 2703(c) may be fairly construed to provide for 'warrant procedures' to be followed when the government seeks customer records that may be protected under the Fourth Amendment, including historical cell site location information." *Fifth Circuit CSLI Opinion*, 724 F.3d at 617 (Dennis, J., dissenting). The determination that "one proposed interpretation or use of the SCA as applied did not comply with the Fourth Amendment's requirement for a warrant based on probable cause" is firmly within the purview of the judiciary. Pet. App. 32a (Stranch, J., concurring). Indeed, "[t]he question before [the court] is one that courts routinely answer: did the search at issue require a warrant?" *Id.* at 31a–32a. This Court should provide a "simple" answer—"get a warrant." *Riley*, 134 S. Ct. at 2495.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully Submitted,

Nathan Freed Wessler
Counsel of Record
Ben Wizner
Steven R. Shapiro
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

Harold Gurewitz
GUREWITZ & RABEN, PLC
333 W. Fort Street,
Suite 1400
Detroit, MI 48226

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
AMERICAN CIVIL LIBERTIES
UNION FUND OF
MICHIGAN
2966 Woodward Ave.
Detroit, MI 48201

Dated: September 26, 2016

APPENDIX

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

United States of America,

Plaintiff-Appellee,

v.

No. Nos. 14-1572/1805

Timothy Ivory Carpenter (14-1572);
Timothy Michael Sanders (14-1805),

Defendants-Appellants.

Appeal from the United States District Court
For the Eastern District of Michigan at Detroit.
No. 2:12-cr-20218— Sean F. Cox, District Judge.

Argued: October 14, 2015

Decided and Filed: April 13, 2016

Before: GUY, KETHLEDGE, and STRANCH, Circuit Judges.

COUNSEL

ARGUED: Nathan Freed Wessler, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York, for Amicus Curiae. Harold Gurewitz, GUREWITZ & RABEN, PLC, Detroit, Michigan, for Appellant in 14-1572. Evan Howard Caminker, UNITED STATES ATTORNEY'S OFFICE, Detroit, Michigan, for Appellee. **ON BRIEF:** Harold Gurewitz, GUREWITZ & RABEN, PLC, Detroit, Michigan, for Appellant in

14-1572. S. Allen Early, LAW OFFICE OF S. ALLEN EARLY, Detroit, Michigan, for Appellant in 14-1805. Evan Howard Caminker, UNITED STATES ATTORNEY'S OFFICE, Detroit, Michigan, for Appellee. Nathan Freed Wessler, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York, Daniel S. Korobkin, Michael J. Steinberg, AMERICAN CIVIL LIBERTIES UNION FUND OF MICHIGAN, Detroit, Michigan, Rachel Levinson-Waldman, Michael W. Price, BRENNAN CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL OF LAW, New York, New York, for Amicus Curiae.

KETHLEDGE, J., delivered the opinion of the court in which GUY, J., joined. STRANCH, J., joined the opinion in part and the result in part. STRANCH, J. (pp. 17–22), delivered a separate opinion joining in Parts II.B and III of the majority opinion and concurring in the judgment only with respect to Part II.A.

OPINION

KETHLEDGE, Circuit Judge. In Fourth Amendment cases the Supreme Court has long recognized a distinction between the content of a communication and the information necessary to convey it. Content, per this distinction, is protected under the Fourth Amendment, but routing information is not. Here, Timothy Carpenter and Timothy Sanders were convicted of nine armed robberies in violation of the Hobbs Act. The

government's evidence at trial included business records from the defendants' wireless carriers, showing that each man used his cellphone within a half-mile to two miles of several robberies during the times the robberies occurred. The defendants argue that the government's collection of those records constituted a warrantless search in violation of the Fourth Amendment. In making that argument, however, the defendants elide both the distinction described above and the difference between GPS tracking and the far less precise locational information that the government obtained here. We reject the defendants' Fourth Amendment argument along with numerous others, and affirm the district court's judgment.

I.

In April 2011, police arrested four men suspected of committing a string of armed robberies at Radio Shacks and T-Mobile stores in and around Detroit. One of the men confessed that the group had robbed nine different stores in Michigan and Ohio between December 2010 and March 2011, supported by a shifting ensemble of 15 other men who served as getaway drivers and lookouts. The robber who confessed to the crimes gave the FBI his own cellphone number and the numbers of other participants; the FBI then reviewed his call records to identify still more numbers that he had called around the time of the robberies.

In May and June 2011, the FBI applied for three orders from magistrate judges to obtain "transactional records" from various wireless carriers for 16 different phone numbers. As part of those applications, the FBI recited that these records

included "[a]ll subscriber information, toll records and call detail records including listed and unlisted numbers dialed or otherwise transmitted to and from [the] target telephones from December 1, 2010 to present[,]" as well as "cell site information for the target telephones at call origination and at call termination for incoming and outgoing calls[.]" The FBI also stated that these records would "provide evidence that Timothy Sanders, Timothy Carpenter and other known and unknown individuals" had violated the Hobbs Act, 18 U.S.C. § 1951. The magistrates granted the applications pursuant to the Stored Communications Act, under which the government may require the disclosure of certain telecommunications records when "specific and articulable facts show[] that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

The government later charged Carpenter with six counts, and Sanders with two, of aiding and abetting robbery that affected interstate commerce, in violation of the Hobbs Act, and aiding and abetting the use or carriage of a firearm during a federal crime of violence. *See* 18 U.S.C. §§ 924(c), 1951(a). Before trial, Carpenter and Sanders moved to suppress the government's cell-site evidence on Fourth Amendment grounds, arguing that the records could be seized only with a warrant supported by probable cause. The district court denied the motion.

At trial, seven accomplices testified that Carpenter organized most of the robberies and often supplied the guns. They also testified that Carpenter and his half-brother Sanders had served as lookouts during the robberies. According to these witnesses, Carpenter typically waited in a stolen car across the street from the targeted store. At his signal, the robbers entered the store, brandished their guns, herded customers and employees to the back, and ordered the employees to fill the robbers' bags with new smartphones. After each robbery, the team met nearby to dispose of the guns and getaway vehicle and to sell the stolen phones.

FBI agent Christopher Hess offered expert testimony regarding the cell-site data provided by Carpenter's and Sanders's wireless carriers, MetroPCS and T-Mobile. Hess explained that cellphones work by establishing a radio connection with nearby cell towers (or "cell sites"); that phones are constantly searching for the strongest signal from those towers; and that individual towers project different signals in each direction or "sector," so that a cellphone located on the north side of a cell tower will use a different signal than a cellphone located on the south side of the same tower. Hess said that cell towers are typically spaced widely in rural areas, where a tower's coverage might reach as far as 20 miles. In an urban area like Detroit, however, each cell site covers "typically anywhere from a half-mile to two miles." He testified that wireless carriers typically log and store certain call-detail records of their customers' calls, including the date, time, and length of each call; the phone numbers engaged on the call; and the cell sites

where the call began and ended.

With the cell-site data provided by Carpenter's and Sanders's wireless carriers, Hess created maps showing that Carpenter's and Sanders's phones were within a half-mile to two miles of the location of each of the robberies around the time the robberies happened. Hess used MetroPCS call-detail records, for example, to show that Carpenter was within that proximity of a Detroit Radio Shack that was robbed around 10:35 a.m. on December 13, 2010. Specifically, MetroPCS records showed that at 10:24 a.m. Carpenter's phone received a call that lasted about four minutes. At the start and end of the call, Carpenter's phone drew its signal from MetroPCS tower 173, sectors 1 and 2, located southwest of the store and whose signals point north-northeast. After the robbery, Carpenter placed an eight-minute call originating at tower 145, sector 3, located northeast of the store, its signal pointing southwest; when the call ended, Carpenter's phone was receiving its signal from tower 164, sector 1, alongside Interstate 94, north of the Radio Shack. *See* Carpenter App'x at 11. Hess provided similar analysis concerning the locations of Carpenter's and Sanders's phones at the time of a December 18, 2010 robbery in Detroit; a March 4, 2011 robbery in Warren, Ohio; and an April 5, 2011 robbery in Detroit. *See* Carpenter App'x at 12-15.

The jury convicted Carpenter and Sanders on all of the Hobbs Act counts and convicted Carpenter on all but one of the § 924(c) gun counts. Carpenter's convictions on the § 924(c) counts subjected him to four mandatory-minimum prison sentences of 25 years, each to be served

consecutively, leaving him with a Sentencing Guidelines range of 1,395 to 1,428 months' imprisonment. The district court sentenced Carpenter to 1,395 months' imprisonment and Sanders to 170 months' imprisonment. Carpenter and Sanders now appeal their convictions and sentences.

II.

A.

Carpenter and Sanders challenge the district court's denial of their motion to exclude their cell-site data from the evidence at trial. Those data themselves took the form of business records created and maintained by the defendants' wireless carriers: when the defendants made or received calls with their cellphones, the phones sent a signal to the nearest cell-tower for the duration of the call; the providers then made records, for billing and other business purposes, showing which towers each defendant's phone had signaled during each call. The government thereafter collected those records, and hence these cell-site data, for a range of dates (127 days of records for Carpenter, 88 days for Sanders) encompassing the robberies at issue here. The government did so pursuant to a court order issued under the Stored Communications Act, which required the government to show "reasonable grounds" for believing that the records were "relevant and material to an ongoing investigation." 18 U.S.C. § 2703(d). Carpenter and Sanders argue that the Fourth Amendment instead required the government to obtain a search warrant, pursuant to a showing of probable cause,

before collecting the data. The district court rejected that argument, holding that the government's collection of cell-site records created and maintained by defendants' wireless carriers was not a search under the Fourth Amendment. We review the district court's decision de novo. *See United States v. Lee*, 793 F.3d 680, 684 (6th Cir. 2015).

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures[.]" U.S. Const. amend. IV. "[F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates." *United States v. Jones*, 132 S.Ct 945, 950 (2012). Government trespasses upon those areas normally count as a search. *Id.* In *Katz v. United States*, 389 U.S. 347 (1967), however, the Supreme Court moved beyond a property-based understanding of the Fourth Amendment, to protect certain expectations of privacy as well. To fall within these protections, an expectation of privacy must satisfy "a twofold requirement": first, the person asserting it must "have exhibited an actual (subjective) expectation of privacy"; and second, that expectation must "be one that society is prepared to recognize as 'reasonable.'" *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). When an expectation of privacy meets both of these requirements, government action that "invade[s]" the expectation normally counts as a search. *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

This case involves an asserted privacy interest in information related to personal communications. As to that kind of information, the federal courts have long recognized a core distinction: although the content of personal communications is private, the information necessary to get those communications from point A to point B is not. For example, in *Ex parte Jackson*, 96 U.S. 727, 733 (1878), the Court held that postal inspectors needed a search warrant to open letters and packages, but that the "outward form and weight" of those mailings— including, of course, the recipient's name and physical address—was not constitutionally protected. *Id.* That was true even though that information could sometimes bring embarrassment: "In a small village, for instance, a young gentleman may not altogether desire that all the loungers around the store which contains the Post-office shall be joking about the fair object of his affections." *Our Letters*, N.Y. Times, Dec. 12, 1872, at 4.

In the twentieth century, the telephone call joined the letter as a standard form of communication. The law eventually followed, recognizing that police cannot eavesdrop on a phone call—even a phone call placed from a public phone booth—without a warrant. *See Katz*, 389 U.S. at 352-55. But again the Supreme Court distinguished between a communication's content and the information necessary to send it. In *Katz*, the Court held that "[t]he Government's activities in electronically listening to and recording the petitioner's *words*" was a search under the Fourth Amendment. *Id.* at 353 (emphasis added). But in *Smith*, the Court held that the police's installation of

a pen register—a device that tracked the phone numbers a person dialed from his home phone—was not a search because the caller could not reasonably expect those numbers to remain private. "Although [the caller's] conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed." *Smith*, 442 U.S. at 743 (emphasis in original).

Today, the same distinction applies to internet communications. The Fourth Amendment protects the content of the modern-day letter, the email. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). But courts have not (yet, at least) extended those protections to the internet analogue to envelope markings, namely the metadata used to route internet communications, like sender and recipient addresses on an email, or IP addresses. *See, e.g., United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010); *United States v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir. 2008); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007).

The business records here fall on the unprotected side of this line. Those records say nothing about the content of any calls. Instead the records include routing information, which the wireless providers gathered in the ordinary course of business. Carriers necessarily track their customers' phones across different cell-site sectors to connect and maintain their customers' calls. And carriers keep records of these data to find weak spots in their network and to determine whether roaming charges apply, among other purposes. Thus,

the cell-site data –like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves. The government's collection of business records containing these data therefore is not a search.

The Supreme Court's decision in *Smith* confirms the point. At the outset, the Court observed that Smith could not claim that "his 'property' was invaded" by the State's actions, which meant he could not claim any property-based protection under the Fourth Amendment. And as to privacy, the Court hewed precisely to the content-focused distinction that we make here. 442 U.S. at 741. The Court emphasized (literally) that the State's pen register did "not acquire the *contents* of communications." *Id.* (emphasis in original). Instead, the Court observed, the phone numbers acquired by the State had been dialed "as a means of establishing communication." *Id.* Moreover, the Court pointedly refused to adopt anything like a "least- sophisticated phone user" (to paraphrase the Fair Debt Collection Practices Act) standard in determining whether phone users know that they convey that information to the phone company: "All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id.* at 742. The Court likewise charged "telephone users" with knowledge that "the phone company has facilities for recording" numerical information and that "the phone company does in fact record this information for a variety of legitimate business purposes." *Id.* at

743. Thus, the Court held, Smith "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business." 442 U.S. at 744. Hence the numerical information was not protected under the Fourth Amendment.

The same things are true as to the locational information here. The defendants of course lack any property interest in cell-site records created and maintained by their wireless carriers. More to the point, when the government obtained those records, it did "not acquire the *contents* of communications." *Id.* at 741. Instead, the defendants' cellphones signaled the nearest cell towers—thereby giving rise to the data obtained by the government here—solely "as a means of establishing communication." *Id.* Moreover, any cellphone user who has seen her phone's signal strength fluctuate must know that, when she places or receives a call, her phone "exposes" its location to the nearest cell tower and thus to the company that operates the tower. *Accord United States v. Davis*, 785 F.3d 498, 511 (11th Cir. 2015) (en banc); *In re Application for Historical Cell Site Data*, 724, F.3d 600, 614 (5th Cir. 2013). And any cellphone user who has paid "roaming" (*i.e.*, out-of-network) charges—or even cellphone users who have not— should know that wireless carriers have "facilities for recording" locational information and that "the phone company does in fact record this information for a variety of legitimate business purposes." *Id.* at 743. Thus, for the same reasons that Smith had no expectation of privacy in the numerical information at issue there, the defendants have no such expectation in the locational information here. On this point, *Smith* is

binding precedent.

The defendants and their amicus, the American Civil Liberties Union, argue that *Jones* liberates us to hold otherwise. In *Jones*, five Justices (though not the Court in its majority opinion) agreed that "longer term GPS monitoring in government investigations of most offenses impinges on expectations of privacy." 132 S. Ct. at 964 (Alito, J., concurring in the judgment); *id.* at 955 (Sotomayor, J., concurring) (same). But there are at least two problems with the defendants' argument as made here. The first is that the government action in this case is very different from the government action in *Jones*. That distinction matters: in applying *Katz*, "it is important to begin by specifying *precisely the nature of the state activity that is challenged*." *Smith*, 442 U.S. at 741 (emphasis added). Whether a defendant had a legitimate expectation of privacy in certain information depends in part on what the government did to get it. A phone conversation is private when overheard by means of a wiretap; but that same conversation is unprotected if an agent is forced to overhear it while seated on a Delta flight. Similarly, information that is not particularly sensitive—say, the color of a suspect's vehicle—might be protected if government agents broke into the suspect's garage to get it. Yet information that is highly sensitive—say, all of a suspect's credit-charges over a three-month period—is not protected if the government gets that information through business records obtained per a subpoena. *See United States v. Phibbs*, 999 F.2d 1053, 1077-78 (6th Cir. 1993).

This case involves business records obtained from a third party, which can only diminish the defendants' expectation of privacy in the information those records contain. *See United States v. Miller*, 425 U.S. 435, 443 (1976); *Phibbs*, 999 F.2d at 1077-78. *Jones*, in contrast, lands near the other end of the spectrum: there, government agents secretly attached a GPS device to the underside of Jones's vehicle and then monitored his movements continuously for four weeks. That sort of government intrusion presents one set of Fourth Amendment questions; government collection of business records presents another. And the question presented here, as shown above, is answered by *Smith*.

The second problem with the defendants' reliance on *Jones* is that—unlike *Jones* this is not a GPS-tracking case. GPS devices are accurate within about 50 feet, which is accurate enough to show that the target is located within an individual building. Data with that kind of accuracy might tell a story of trips to "the strip club, the criminal defense attorney, the by-the- hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on[.]" *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (internal quotation marks omitted). But here the cell-site data cannot tell that story. Instead, per the undisputed testimony at trial, the data could do no better than locate the defendants' cellphones within a 120- (or sometimes 60-) degree radial wedge extending between one-half mile and two miles in length. Which is to say the locational data here are accurate within a 3.5 million square-foot to 100 million square-foot area—as much as 12,500 times less accurate than the

GPS data in *Jones*. And cell phone locational data are even less precise in suburban and rural settings. Areas of this scale might encompass bridal stores and Bass Pro Shops, gay bars and straight ones, a Methodist church and the local mosque. The ACLU responds that so-called "femtocells" can provide service (and thus identify a phone's location) within areas as small as ten meters. But our task is to decide this case, not hypothetical ones; and in this case there are no femtocells to be found. The defendants' argument is without merit.

The defendants similarly rely on *Riley v. California*, 134 S. Ct 2473, 2485 (2014), where the Court held the government may not access a smartphone's internal data - or, one might say, its contents -- without a warrant. But the Court's rationale was that smartphones typically store vast amounts of information about their users—vastly more, of course, than whether the user happens to be located within a two-mile radial wedge. *Riley* only illustrates the core distinction we make here.

Some other points bear mention. One is that Congress has specifically legislated on the question before us today, and in doing so has struck the balance reflected in the Stored Communications Act. The Act stakes out a middle ground between full Fourth Amendment protection and no protection at all, requiring that the government show "reasonable grounds" but not "probable cause" to obtain the cell-site data at issue here. *See* 18 U.S.C. § 2703(d). The defendants and the ACLU effectively ask us to declare that balance unconstitutional. There is considerable irony in that request. The *Katz* standard asks whether the defendants' asserted

expectation of privacy "is 'one that society is prepared to recognize as reasonable[.]'" *Smith*, 442 U.S. at 740 (quoting *Katz*, 389 U.S. at 361). Here, one might say that society itself—in the form of its elected representatives in Congress—has already struck a balance that it thinks reasonable. That is not to say that courts should defer to Congress's judgment on constitutional questions. But when the question itself turns on society's views, and society has in a meaningful way already expressed them, judges should bring a certain humility to the task of deciding whether those views are reasonable—lest judges "confuse their own expectations of privacy," *Jones*, 132 S. Ct. at 962 (Alito, J., concurring), with those that every reasonable person must hold.

A second point is related. Constitutional judgments typically rest in part on a set of empirical assumptions. When those assumptions concern subjects that judges know well—say, traffic stops—courts are well-equipped to make judgments that strike a reasonable balance among the competing interests at stake. *See* Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case For Caution, 102 Mich. L. Rev. 801, 863 (2004). But sometimes new technologies—say, the latest iterations of smartphones or social media—evolve at rates more common to superbugs than to large mammals. In those situations judges are less good at evaluating the empirical assumptions that underlie their constitutional judgments. Indeed the answers to those empirical questions might change as quickly as the technology itself does. With regard to the *Katz* test in particular, for example, "[d]ramatic

technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes." *Jones*, 132 S. Ct. at 962 (Alito, J., concurring). Congress is usually better equipped than courts are to answer the empirical questions that such technologies present. Thus, "[w]hen technologies are new and their impact remains uncertain, statutory rules governing law enforcement powers will tend to be more sophisticated, comprehensive, forward-thinking, and flexible than rules created by the judicial branch." Kerr, 102 Mich. L. Rev. at 859-60. These concerns favor leaving undisturbed the Congressional judgment here.

In sum, we hold that the government's collection of business records containing cell-site data was not a search under the Fourth Amendment.

B.

Sanders argues that the district court should have suppressed the government's cell-site evidence for another reason, namely that (in his view) the government's applications to obtain the cell-site records failed to show "reasonable grounds" for believing that the records were "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). There are several problems with that argument, but the simplest is that suppression of evidence is not among the remedies available under the Stored Communications Act. Quite the contrary: the statute identifies a handful of civil remedies, including "damages" and "equitable or declaratory relief," 18 U.S.C. § 2707(b), and

provides that those "are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708; *see United States v. Guerrero*, 768 F.3d 351, 358 (5th Cir. 2014). The relief that Sanders seeks is therefore unavailable under the Act. *See United States v. Abdi*, 463 F.3d 547, 556 (6th Cir. 2006).

III.

A.

Carpenter argues that the district court erred when it denied Carpenter's motion for acquittal for lack of venue over counts seven and eight. Those counts charged Carpenter with aiding and abetting a Hobbs Act robbery in Warren, Ohio, and with aiding and abetting the use of a firearm in connection with that robbery. *See* 18 U.S.C. §§ 924(c), 1951(a). We review the district court's decision de novo. *See United States v. Kuehne*, 547 F.3d 667, 677 (6th Cir. 2008).

Carpenter was prosecuted in the Eastern District of Michigan. Venue was proper there so long as a rational trier of fact, viewing the evidence in the light most favorable to the government, could find by a preponderance of the evidence that any of Carpenter's accessorial acts, or the underlying crime itself, occurred in the Eastern District of Michigan. Relatedly, "[w]here venue is appropriate for the underlying crime of violence, so too it is for the § 924(c)(1) offense." *United States v. Rodriguez-Moreno*, 526 U.S. 275, 282 (1999).

Here, Carpenter's accomplices testified that, while in the Eastern District of Michigan,

Carpenter recruited the robbers for the Warren robbery, described for them the robbery's general scheme, and from there drove them to Ohio. Two of these witnesses also testified that, while in Michigan, Carpenter made arrangements to have another accomplice supply the robbers with a gun when they got to Warren. A reasonable trier of fact could credit this testimony, and conclude that much of Carpenter's conduct in abetting both the Warren robbery and the use of a firearm during it took place in the Eastern District of Michigan. The district court correctly denied Carpenter's motion for acquittal on counts seven and eight.

B.

Carpenter argues that the district court should have allowed him to use a report prepared by FBI Special Agent Vicente Ruiz to refresh the memory of government witness Adriane Foster on cross-examination. We review that evidentiary ruling for an abuse of discretion. *See United States v. Morales*, 687 F.3d 697, 701 (6th Cir. 2012).

At trial, Carpenter's counsel cross-examined Foster—an accomplice of Carpenter - about Foster's past statements to Agent Ruiz. Foster testified that he told Ruiz that Carpenter had provided Foster with advance information about the robbery in Warren. According to Ruiz's written summary of the interview, however, Foster told Ruiz that Sanders, not Carpenter, had provided Foster with advance information about the robbery. Carpenter's counsel sought to introduce Ruiz's report to "refresh [Foster's] memory" of the interview.

A document may be used to refresh a witness's memory only after his memory has been "exhausted." *Rush v. Ill. Cent. R.R. Co.*, 399 F.3d 705, 716 (6th Cir. 2005). Here, Foster seemed to have no trouble remembering his conversation with Agent Ruiz. Foster repeatedly testified that he did remember telling Ruiz that Timothy Carpenter—not Timothy Sanders—had told him about the plans for the Warren robbery. Carpenter's counsel then asked Foster whether he remembered "saying something different" to Ruiz. Foster said that he did not. That answer did not show that Foster's memory needed refreshing; it showed that Foster disagreed with Carpenter about what Foster had told Ruiz. What Carpenter actually sought to do with the report was not refresh Ruiz's memory, but impeach his testimony. The district court did not abuse its discretion in ruling that Carpenter could not use the report for that purpose.

To the same end, Carpenter argues that the district court should have allowed him to introduce Ruiz's report as extrinsic evidence of a prior inconsistent statement under Federal Rule of Evidence 613(b). But an FBI agent's written summary of an interview with a declarant cannot be used to impeach the declarant's later testimony unless the declarant has attested to the report's accuracy. *See United States v. Barile*, 286 F.3d 749, 757 (4th Cir. 2002); *United States v. Schoenborn*, 4 F.3d 1424, 1429 & n.3 (7th Cir. 1993). Foster has not done that here; to the contrary, Foster testified that Ruiz's report would have been wrong if it said that Sanders rather than Carpenter had told him about the plans for the Warren robbery. The district court thus correctly

barred the report's introduction at trial.

C.

1.

Carpenter's remaining argument is that his 1,395-month sentence is so disproportionate to his crimes as to violate the Eighth Amendment's prohibition on cruel and unusual punishment. He also argues that his mandatory-minimum sentences for his § 924(c) convictions violate the constitutional separation of powers. We consider both issues de novo. *See United States v. Kelsor*, 665 F.3d 684, 701 (6th Cir. 2011).

"[O]nly an extreme disparity between crime and sentence offends the Eighth Amendment." *United States v. Odeneal*, 517 F.3d 406, 414 (6th Cir. 2008). In *Solem v. Helm*, 463 U.S. 277 (1983), the Supreme Court held that the Eighth Amendment prohibited a state court from sentencing to life imprisonment without parole a recidivist criminal who wrote a bad check for $100. But in *Ewing v. California*, 538 U.S. 11 (2003), the Supreme Court rejected the Eighth Amendment claim of a defendant who was sentenced to 25 years to life for stealing several golf clubs. 538 U.S. at 28-30.

Carpenter has a long criminal history. In this case, as the district court observed, Carpenter organized and led several "very violent" robberies that put his victims "in extreme danger[.]" Meanwhile, in other armed-robbery cases, we have already held that sentences even longer than Carpenter's were constitutionally permissible. *See United States v. Clark*, 634 F.3d 874, 877-78

(6th Cir. 2011) (2,269 months); *United States v. Watkins*, 509 F.3d 277, 282 (6th Cir. 2007) (1,772 months). Carpenter's sentence does not violate the Eighth Amendment.

Nor do his mandatory-minimum sentences violate the constitutional separation of powers. "Congress has the power to define criminal punishments without giving the courts any sentencing discretion." *Chapman v. United States*, 500 U.S. 453, 467 (1991). Carpenter acknowledges that we have "flatly rejected" his argument in other cases. Carpenter Br. at 54; *see, e.g., United States v. Cecil*, 615 F.3d 678, 696 (6th Cir. 2010). This case is no different.

2.

Sanders challenges his sentence on non-constitutional grounds, arguing that the district court misapplied the Sentencing Guidelines and that his sentence is "greater than necessary" to accomplish the remedial objectives of incarceration. *See* 18 U.S.C. § 3553. We review for clear error the district court's factual findings in support of Sanders's sentence, and review the sentence itself for an abuse of discretion. *See United States v. Randolph*, 794 F.3d 602, 614 (6th Cir. 2015).

Sanders argues first that the district court incorrectly applied sentencing enhancements for brandishing or possessing a firearm in furtherance of robbery, and for physically restraining a person in furtherance of a robbery. *See* U.S.S.G. §§ 2B3.1(b)(2)(C), (b)(4)(B). Sanders himself need not have committed those acts in order for the enhancements to apply; rather, he need only have

known it was "reasonably probable" that a co-participant would commit them. *See United States v. Woods*, 604 F.3d 286, 291 (6th Cir. 2010).

That standard is met here. During the January 7, 2011 robbery, Sanders's accomplice Juston Young returned to the getaway car with gun in hand. Thus, when Sanders teamed up with Young and others for another robbery on March 4, Sanders could have easily foreseen that Young would brandish a firearm in the course of the crime—as in fact Young did. The district court did not clearly err in finding that the firearm enhancement applied to Sanders.

Nor did the court err in finding that Sanders could foresee that Young would physically restrain someone during the March 4 robbery. As a general matter, an accomplice to robbery should foresee that robbery likely entails physical restraint or worse. *See* U.S. Sentencing Guidelines Manual § 1B1.3 cmt. n.2 (2012). And Sanders knew specifically that the plan for that robbery was for the robbers to move customers and employees to the back of the store. The physical-restraint enhancement was therefore proper. That leaves an enhancement for brandishing a firearm during the January 7 robbery. But that enhancement had no effect on Sanders's Guidelines range: the offense level for the March 4 robbery was higher than the offense level for the January 7 robbery, even with the brandishing enhancement; and the offense level for the March 4 robbery, not the January 7 one, thus determined his total offense level under the Guidelines. Any error as to the brandishing enhancement for the January 7 robbery was

therefore harmless. *See United States v. Jeross*, 521 F.3d 562, 574-76 (6th Cir. 2008).

Finally, the district court acted within its discretion in sentencing Sanders to 170 months' imprisonment, which fell squarely within his Guidelines range of 151 to 188 months. Within-Guidelines sentences are presumptively reasonable in this circuit. *See United States v. Kamper*, 748 F.3d 728, 739-40 (6th Cir. 2014). Moreover, the district court considered and rejected the arguments that Sanders raised at his sentencing hearing, and otherwise properly determined that the sentence was appropriate in light of 18 U.S.C. § 3553(a). The court did not abuse its discretion.

* * *

The judgments in both cases are affirmed.

CONCURRENCE

STRANCH, Circuit Judge, concurring. I join Parts II.B and III of the majority opinion, which resolve Carpenter's and Sanders's statutory, evidentiary, and sentencing claims. I concur only in the judgment with respect to Part II.A because I believe that the sheer quantity of sensitive information procured without a warrant in this case raises Fourth Amendment concerns of the type the Supreme Court and our circuit acknowledged in *United States v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring), and in *United States v. Skinner*, 690 F.3d 772, 780 (6th Cir. 2012). Though

I write to address those concerns, particularly the nature of the tests we apply in this rapidly changing area of technology. I find it unnecessary to reach a definitive conclusion on the Fourth Amendment issue. I concur with the majority on the basis that were there a Fourth Amendment violation, I would hold that the district court's denial of Carpenter and Sanders's motion to suppress was nevertheless proper because some extension of the good-faith exception to the exclusionary rule would be appropriate.

A. Fourth Amendment Concerns

At issue here is not whether the cell-site location information (CSLI) for Carpenter and Sanders could have been obtained under the Stored Communications Act (SCA). The question is whether it should have been sought through provisions of the SCA directing the government to obtain a warrant with a probable cause showing, 18 U.S.C. § 2703(c)(1)(A), or a court order based on the specified "reasonable grounds[,]" *id.* §§ 2703(c)(1)(B), (d). This leads us to the requirements of the Fourth Amendment.

Fourth Amendment law was complicated in the time of paper correspondence and land phone lines. The addition of cellular (not to mention internet) communication has left courts struggling to determine if (and how) existing tests apply or whether new tests should be framed. I am inclined to favor the latter approach for several reasons, particularly one suggested by Justice Sotomayor: "[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of

privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (citations omitted).

It is easier to see why the existing tests present problems than it is to articulate a test that will not. This difficulty is exemplified by the two conceptual categories under the Fourth Amendment found in this case and the law that governs each. The majority accurately describes two different strains of law, one addressing the distinction between GPS tracking and the less accurate CSLI obtained and used in this case and the other "between the content of a communication and the information necessary to convey it." (Majority Op. at 2.) To understand whether and how the tests established in these two different strains of Fourth Amendment law might apply requires a brief review of each.

First, the distinction between GPS tracking and CSLI acquisition. CSLI does appear to provide significantly less precise information about a person's whereabouts than GPS and, consequently, I agree that a person's privacy interest in the CSLI his or her cell phone generates may indeed be lesser. *See, e.g.*, *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."); *id.* at 963 (Alito,

J., concurring) ("For older phones, the accuracy of the location information depends on the density of the tower network, but new 'smart phones,' which are equipped with a GPS device, permit more precise tracking.").

But precision is not the only variable with legal significance. In *United States v. Skinner*, we addressed the government's use of GPS data emitted by a suspect's cell phone to track the suspect's whereabouts over the course of three days. *Skinner*, 690 F.3d at 774–76. The tracking took place pursuant to a court order authorizing the suspect's phone company to provide the government access to the GPS data emitted by the suspect's pay-as-you-go cell phone. *See id.* at 776. The majority opinion there acknowledged "the concern raised by Justice Alito's concurrence in *Jones*" that long-term location monitoring in government investigations impinges on expectations of privacy, but held that the concern was not implicated in Skinner's case because of the relatively short tracking period. *Id.* at 780. It distinguished *Jones*, explaining that "[w]hile *Jones* involved intensive monitoring over a 28-day period, here the DEA agents only tracked Skinner's cell phone for three days. Such 'relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable.'" *Id.* (quoting *Jones*, 132 S. Ct. at 964 (Alito, J., concurring)). But *Skinner* framed this conclusion with a key caveat: "There may be situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes." *Id.*

Primarily analyzing this case under the tests established for the assertion of a privacy interest in business records, the majority here determines that the CSLI is unprotected because it deals with routing or conveying information, not the content of the related communications. (Majority Op. at 6–8.) This analysis reflects a valid distinction in that arena of the law. It is here, however, that my concern arises with the existing tests. It seems to me that our case resides at the intersection of the law governing tracking of personal location and the law governing privacy interests in business records. This case involves tracking physical location through cell towers and a personal phone, a device routinely carried on the individual's person; it also involves the compelled provision of records that reflect such tracking. In light of the personal tracking concerns articulated in our precedent, I am not convinced that the situation before us can be addressed appropriately with a test primarily used to obtain business records such as credit card purchases –records that do not necessarily reflect personal location. And it seems to me that the business records test is ill suited to address the issues regarding personal location that are before us. I therefore return to the law governing location.

I begin by acknowledging that this case involves CSLI that does not reach the specificity of GPS. Nonetheless, *Skinner* recognizes "situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes." *Skinner*, 690 F.3d at 780. The tracking of cell-phone data in this case went far beyond 3 or even

28 days—the government procured approximately 127 days of CSLI records for Carpenter and 88 days for Sanders. That is close to four and three months, respectively. Even taking into account the less precise nature of CSLI as compared to GPS, such extensive monitoring far exceeds the threshold we identified in *Skinner* and the warrantless acquisition of such substantial quantities of CSLI implicates the *Skinner*/*Jones* concerns. I do not think that treating the CSLI obtained as a "business record" and applying that test addresses our circuit's stated concern regarding long-term, comprehensive tracking of an individual's location without a warrant. At issue here is neither relatively innocuous routing information nor precise GPS locator information: it is personal location information that partakes of both. I am also concerned about the applicability of a test that appears to admit to no limitation on the quantity of records or the length of time for which such records may be compelled. I conclude that our precedent suggests the need to develop a new test to determine when a warrant may be necessary under these or comparable circumstances.

B. The Exclusionary Rule & Good-Faith Exception

"When evidence is obtained in violation of the Fourth Amendment, the judicially developed exclusionary rule usually precludes its use in a criminal proceeding against the victim of the illegal search and seizure." *Illinois v. Krull*, 480 U.S. 340, 347 (1987). The exclusionary rule is not intended "to redress the injury to the privacy of the search victim[.] . . . Instead, the rule's prime purpose is to

Primarily analyzing this case under the tests established for the assertion of a privacy interest in business records, the majority here determines that the CSLI is unprotected because it deals with routing or conveying information, not the content of the related communications. (Majority Op. at 6–8.) This analysis reflects a valid distinction in that arena of the law. It is here, however, that my concern arises with the existing tests. It seems to me that our case resides at the intersection of the law governing tracking of personal location and the law governing privacy interests in business records. This case involves tracking physical location through cell towers and a personal phone, a device routinely carried on the individual's person; it also involves the compelled provision of records that reflect such tracking. In light of the personal tracking concerns articulated in our precedent, I am not convinced that the situation before us can be addressed appropriately with a test primarily used to obtain business records such as credit card purchases—records that do not necessarily reflect personal location. And it seems to me that the business records test is ill suited to address the issues regarding personal location that are before us. I therefore return to the law governing location.

I begin by acknowledging that this case involves CSLI that does not reach the specificity of GPS. Nonetheless, *Skinner* recognizes "situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes." *Skinner*, 690 F.3d at 780. The tracking of cell-phone data in this case went far beyond 3 or even

28 days—the government procured approximately 127 days of CSLI records for Carpenter and 88 days for Sanders. That is close to four and three months, respectively. Even taking into account the less precise nature of CSLI as compared to GPS, such extensive monitoring far exceeds the threshold we identified in *Skinner* and the warrantless acquisition of such substantial quantities of CSLI implicates the *Skinner*/*Jones* concerns. I do not think that treating the CSLI obtained as a "business record" and applying that test addresses our circuit's stated concern regarding long-term, comprehensive tracking of an individual's location without a warrant. At issue here is neither relatively innocuous routing information nor precise GPS locator information: it is personal location information that partakes of both. I am also concerned about the applicability of a test that appears to admit to no limitation on the quantity of records or the length of time for which such records may be compelled. I conclude that our precedent suggests the need to develop a new test to determine when a warrant may be necessary under these or comparable circumstances.

B. The Exclusionary Rule & Good-Faith Exception

"When evidence is obtained in violation of the Fourth Amendment, the judicially developed exclusionary rule usually precludes its use in a criminal proceeding against the victim of the illegal search and seizure." *Illinois* v. *Krull*, 480 U.S. 340, 347 (1987). The exclusionary rule is not intended "to redress the injury to the privacy of the search victim[.] . . . Instead, the rule's prime purpose is to

deter future unlawful police conduct and thereby effectuate the guarantee of the Fourth Amendment against unreasonable searches and seizures[.]" *United States v. Calandra*, 414 U.S. 338, 347 (1974). "As with any remedial device, application of the exclusionary rule properly has been restricted to those situations in which its remedial purpose is effectively advanced." *Krull*, 480 U.S. at 347.

This restriction has led the Supreme Court to articulate certain "exceptions" to the exclusionary rule. For example, in *United States v. Leon*, 468 U.S. 897 (1984), the Supreme Court held that courts generally should not apply the exclusionary rule to evidence obtained by police officers whose reliance on a search warrant issued by a neutral magistrate was objectively reasonable, even if the warrant was ultimately found to be defective. *See Leon*, 468 U.S. at 905– 26; *see also id.* at 926 ("In the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause."). The Court explained that "when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope[,]" "[p]enalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." *Id.* at 920–21 (footnote omitted). In *Illinois v. Krull*, the Supreme Court extended the good-faith exception articulated in *Leon* to evidence obtained in reasonable reliance on a statute that is subsequently declared

unconstitutional, reasoning "that the greatest deterrent to the enactment of unconstitutional statutes by a legislature is the power of the courts to invalidate such statutes." *Krull*, 480 U.S. at 352; *see also id.* at 349–350.

In the instant case, there is nothing to suggest that the FBI agents who obtained the CSLI of Carpenter and Sanders pursuant to the SCA engaged in any intentional misconduct. Suppressing the CSLI at trial would not have the requisite deterrent effect on future unlawful conduct and application of the exclusionary rule is therefore inappropriate. *See, e.g.*, *United States v. Warshak*, 631 F.3d 266, 333–34 (6th Cir. 2010) (Keith, J., concurring). Assuming without deciding that this situation states a Fourth Amendment violation, I would still affirm the district court's denial of Carpenter and Sanders's motion to suppress on this ground.

C. Judicial Review

One further issue of importance bears mentioning. The majority may be correct that Congress is well positioned to gauge changing public attitudes toward new and evolving technology. This institutional advantage may even weigh in favor of approaching challenges to statutes that balance privacy and public safety interests with some caution. But I do not see this case primarily as a challenge to the constitutionality of the SCA's provisions that authorize the government to seek secured communications through *either* an order *or* a warrant. The question before us is one that courts routinely answer: did the search at issue require a

warrant? That the government sought and obtained an order under the SCA does not immunize that order from challenge on Fourth Amendment grounds. As relevant here, our circuit has already had occasion to weigh the propriety of an order under the SCA and to have found that order wanting. *Warshak* explained that "to the extent that the SCA purports to permit the government to obtain [a subscriber's] emails [from an internet service provider] warrantlessly, the SCA is unconstitutional." *Id.* at 288. I do not read that holding as declaring the balance struck by the SCA unconstitutional. (*See* Majority Op. at 10–11.) *Warshak* simply found that one proposed interpretation or use of the SCA as applied did not comply with the Fourth Amendment's requirement for a warrant based on probable cause. Determining the parameters of the Fourth Amendment is the task of the judiciary. *See United States v. Windsor*, 133 S. Ct. 2675, 2688 (2013) (quoting *Zivotofsky v. Clinton*, 132 S. Ct. 1421, 1427 (2012)). The runaway pace of technological development makes this task more difficult. But the job is ours nonetheless and the circumstances before us lead me to believe that we have more work to do to determine the best methods for assessing the application of the Fourth Amendment in the context of new technology.

No. 14-1572

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

FILED
Jun 29, 2016
Deborah S. Hunt, Clerk

v.

ORDER

TIMOTHY IVORY-CARPENTER,

Defendant-Appellant.

BEFORE: GUY, KETHLEDGE, and STRANCH, Circuit Judges.

The court received a petition for rehearing en banc. The original panel has reviewed the petition for rehearing and concludes that the issues raised in the petition were fully considered upon the original submission and decision of the case. The petition then was circulated to the full court. No judge has requested a vote on the suggestion for rehearing en banc.

Therefore, the petition is denied.

ENTERED BY ORDER OF THE COURT

Deborah S. Hunt, Clerk

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

United States of America,

Plaintiff,

v.

Criminal Case No. 12-20218
Honorable Sean F. Cox

Timothy Ivory Carpenter D-4 and
Timothy Michael Sanders D-11,

Defendants.
_____/

OPINION & ORDER

In this action, multiple Defendants were charged with various counts stemming from a series of robberies at cellular telephone stores. Defendants Timothy Carpenter ("Carpenter") and Timothy Sanders ("Sanders") are proceeding to trial. Defendants have filed the following two motions in limine that are contested by the Government: 1) a motion seeking to suppress cell phone data, as violative of the Fourth Amendment; and 2) a motion seeking to preclude Special Agent Christopher Hess from testifying as an expert witness at trial. As explained in greater detail below, the Court shall DENY both motions.

BACKGROUND

In this action, multiple Defendants were charged with various counts stemming from a series of robberies at cellular telephone stores. Defendants Carpenter and Sanders are proceeding to trial.

The Government does not contend that either Carpenter or Sanders entered the stores during the robberies. Rather, it contends that they "acted as lookouts, getaway drivers, planners and the like." (Govt.'s Trial Br. at 2). One of the robberies occurred in Warren Ohio, while the other six robberies occurred in the Metropolitan Detroit area.

The robberies that will be at issue at trial are those charged in Counts One through Fourteen, which occurred during the time period from December 13, 2010 to December 1, 2012.

On May 2, 2011, and again on June 7, 2011, the Government applied for and obtained court orders under 18 U.S.C. § 2703 for toll records, call detail records, and cell/site section information for several different cell phone numbers, including (313) 579-8507 and (313) 412-6845. (*See* 6/7/11 Order signed by Judge Stephen Murphy, D.E. No. 196-2; 5/2/11 Order signed by Magistrate Judge Michaelson, D.E. No. 221-3). Those Orders state that the Government had "demonstrated to the Court that there are *reasonable grounds to believe* that the information sought is relevant and material to a legitimate law enforcement investigation into possible violations of Title 18, United States Code, § 1951." (*Id.* at 1) (emphasis added).

At trial, the Government intends to present evidence through F.B.I. Special Agent Christopher Hess that, on March 4, 2011, Sanders's cell phone, (313) 579-8507, was located in a geographic area consistent with the robbery charged in Count 7, which occurred in Warren, Ohio. It also intends to present evidence that Carpenter's cell phone, (313) 412-6845, was in various areas consistent with

robberies charged in other Counts.

ANALYSIS

I. Motion to Suppress Cell Phone Data: D.E. 196 (With Joinder in D.E. 214)

In this motion, Defendant Sanders asks the Court to suppress cell phone data for cell phone number (313) 579-8507 because the data was obtained in violation of the Fourth Amendment. He makes two arguments. First, he argues that the "reasonable grounds standard" in the Stored Communications Act, 18 U.S.C. § 2703 *et seq.* ("the Act") is unconstitutional. Second, he argues that the Government did not present sufficient "reasonable grounds" information in order to obtain the order in any event.

Defendant Carpenter filed a "Notice of Joinder" (D.E. No. 214), wherein he stated that he "adopts and joins in Defendant [Sanders's] Motion in Limine To Suppress Cell Phone Data (R196)." In a supplement to that notice, he states that "[e]xcept for the difference in phone numbers referred to in the Order," the same analysis applies. (D.E. No. 216).

A. Should The Data Be Suppressed Because The "Reasonable Grounds Standard" In The Act Unconstitutional?

The parties agree that, under the Act, the standard of proof required for the Court Orders at issue here is as follows:

> (d) Requirements for court order . . . A court order for disclosure . . . shall issue

> only if the governmental entity offers specific and articulable facts showing that there are *reasonable grounds to believe* that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation.

18 U.S.C. § 2703(d) (emphasis added).

Defendants argue that the reasonable grounds standard in the Act is unconstitutional because a cell phone user has a reasonable expectation of privacy in prolonged surveillance data and therefore a probable cause determination should be required. Defendants claim that the Sixth Circuit has not addressed this issue and that lower courts that have addressed the issue have been divided. They rely on: 1) *In re U.S. for Historical Cell Site Data*, 747 F.Supp.2d 827 (S.D. Tex. 2010), wherein the district court held that the warrantless seizure of cell cite records over a period of two months was unreasonable because the phone user has a reasonable expectation of privacy in prolonged surveillance information); and 2) *In re Application of U.S.*, 736 F.Supp.2d 578 (E.D. N.Y. 2010), wherein the district court also held that historical cell site data is protected by the Fourth Amendment. Those district court judges were influenced by case law holding that placing a G.P.S. tracking device on a vehicle requires a warrant.

Sanders's brief, filed on November 21, 2013, indicates that the appeal in *In re Application of U.S.* is still pending (*see* Sanders's Br. at 5), but that is not the case. On July 30, 2013, the Fifth Circuit issued its decision *reversing the lower court's ruling*.

In response to Defendants' motion, the Government notes that Defendants have not directed the Court to a single decision by any United States Court of Appeals, much less the Sixth Circuit, that supports their position. The Government directs the Court to *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012).[1] In that case, the authorities obtained court orders for subscriber information, cell cite information, G.P.S. real-time location, and "ping" data for cell phones. *Id.* at 776. In affirming the district court's ruling denying the defendant's motion to suppress, the Sixth Circuit held that there was "no Fourth Amendment violation because [the defendant] did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone." *Id.* at 777. The *Skinner* court reaffirmed there is no legitimate expectation of privacy in cell site data because the "'cell-site data is simply a proxy'" for the defendant's visually observable location, and a defendant has no legitimate expectation of privacy in his movements along public highways. *Id.* at 779 (quoting *United States v. Forrest*, 355 F.3d 942, 951-52 (6th Cir. 2004)). The *Skinner* decision reflects that the Sixth Circuit views obtaining routine cell phone data quite differently than it does data obtained via a G.P.S. device being placed on a vehicle without a warrant:

---

[1] The Government also contends that if Section 2703(d) were found unconstitutional in this case, the evidence should not be suppressed in any event because the agents relied in good faith on the Act in obtaining the evidence. (Govt.'s Br. at 5) (citing *United States v. Warshak*, 631 F.3d 266, 288-89 (6th Cir. 2010)). The Court agrees that this is an additional basis for denying the motion.

> When criminals use modern technological devices to carry out criminal acts . . . they can hardly complain when the police take advantage of the inherent characteristics of those very devices to catch them. *This is not a case in which the government secretly placed a tracking device in someone's car.*

Id. at 774 (emphasis added).

This Court rejects Defendants' argument that the Act is unconstitutional.

B. Did The Government Present Sufficient Reasonable Grounds?

In this motion, Defendants also make a secondary argument that the Government did not present sufficient reasonable grounds to obtain the orders in any event. (*See* Sanders's Br. at 2, asserting that, "upon information and belief," the order was "obtained in violation of the Act because 'reasonable grounds' were not presented to obtain the Order.").

In response, the Government contends it satisfied the applicable standard. (*See* Govt.'s Br. at 5-6). The Court agrees.

The Order that Sanders challenges is the one issued by Judge Murphy. The Application that requested that order (D.E. No. 221-2) set forth the factual basis for the Government's request and included, among other things, that: 1) there was an ongoing criminal investigation as to a series of armed robberies at Radio Shack and T-Mobile stores in Detroit, Michigan; 2) the Detroit Police Department

has arrested four individuals believed to be involved in the robberies; 3) a cooperating defendant was interviewed, admitted his role as to nine robberies, identified others involved in the robberies, indicated they planned to do additional robberies, and provided his own cell phone number and those of others involved in the robberies; and 4) the cell site records are needed to assist in identifying and locating the other persons involved in the robberies. The application that requested the order challenged by Carpenter is nearly identical. The Court finds that the Applications were supported by specific and articulable facts, and therefore meets the "diminished standard that applies to § 2703(d) applications." *United States v. Warshak*, 631 F.3d 266, 291 (6th Cir. 2010).

Accordingly, the Court shall deny this motion.

II. Motion To Exclude Lay And Expert Testimony: D.E. 211 (Joinder In D.E. 215)

In this motion, filed by Carpenter and joined by Sanders, Defendants ask the Court to enter an order excluding expert testimony regarding the operation of cell towers (i.e., the testimony of Special Agent Hess). They ask the Court to do so on several grounds, which are addressed below.

A. Should The Court Exclude Hess's Report Because It Is Untimely, Unfairly Prejudicial, And Fails To Meet Rule 16 Requirements?

First, Defendants argue that the untimely production of Special Agent Hess's report is unfairly prejudicial and fails to meet the requirements of Fed.

R. Crim. P. 16. (Def.'s Br. at 3). Carpenter asserts that he received the discovery which relates to the testimony of Hess "just three weeks before trial." He contends the tardiness of the report is prejudicial because the subject matter (cell-site analysis) is specialized information and the "last-minute disclosure by the Government leaves the Defendant without the tools to effectively cross-examine SA Hess." (*Id.* at 4). Carpenter also contends that Hess's report is deficient because it does sufficiently explain the bases and reasons for his opinions.

As the Government details in its Response Brief, Defense Counsel has been aware for *at least several months prior to trial* that the Government would seek to present an expert witness in cell-site analysis at trial:

1) On April 15, 2013, the Government filed a Discovery Notice (D.E. No. 89) advising Carpenter that it "intends to introduce at trial testimony from one or more experts in the following areas of expertise: cell tower location analysis" and referencing evidence involving "telephone call records and location data." (*Id.*) (underlining in original);

2) On August 16, 3023, the Government filed an identical notice as to Sanders. (D.E. No. 150);

3) During a Status Conference on October 28, 2013, Defense Counsel stated that they needed Special Agent Hess's report in sufficient time that they could hire their own experts. The Court advised Defense Counsel of the recent case that Judge Borman had involving Hess, wherein another expert was called to rebut his

testimony. On that same day, the Court ordered the Government to provide Defense Counsel with Hess's report no later than November 7, 2013.

4) Neither Defendant filed a motion seeking the report earlier or asking the Court to adjourn the trial date.

5) The Government contends that it met the Court's deadline for providing Hess's report; and

6) On November 22, 2013, Sanders submitted a witness list that identifies his own expert witness, Ryan J. Harmon. Carpenter joined in that witness list.

The Court rejects Defendants' timeliness and unfair prejudice argument based on timeliness arguments.

Defendants also contend that Hess's report does not provide sufficient information as to the bases and reasons for his opinions. That argument is also rejected. Hess's report contains a section titled, "Basic Principals [sic] Utilized In Record Analysis" that explains the underlying technology and how it works. Hess then applied those principles and opined that Defendants were in geographic areas consistent with certain robberies.

B. Should The Court Preclude Hess's Proposed Expert Testimony Under Fed. R. Evid. 702 And *Daubert*?

Next, Defendants ask this Court to preclude the Government from calling Special Agent Hess as an expert at trial, pursuant to Fed. R. Evid. 702 and

Daubert, because his proposed testimony is not sufficiently reliable to qualify as expert testimony.

"District court judges must determine whether an expert's testimony is both relevant and reliable when ruling on its admission." *Clay v. Ford Motor Company*, 215 F.3d 663, 667 (6th Cir. 2000). A trial judge's determinations regarding the admissibility of expert testimony are guided by Fed. R. Evid. 702 and *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

Rule 702 of the Federal Rules of Evidence governs testimony by experts and provides as follows:

> A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
> (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
> (b) the testimony is based on sufficient facts or data;
> (c) the testimony is the product of reliable principles and methods; and
> (d) the expert has reliably applied the principles and methods to the facts of the case.

Fed. R. Evid. 702.

Under *Daubert*, the trial court acts as a "gatekeeper" that ensures that any and all scientific testimony or evidence admitted is not only relevant, but reliable. *Daubert* sets forth a nonexclusive list of

factors relevant to this inquiry: 1) whether the theory or technique can be or has been tested; 2) whether it has been subjected to peer review; 3) whether there is a known or potential rate of error; and 4) whether the theory or technique enjoys general acceptance in the relevant scientific community. *Daubert*, 509 U.S at 593-94. In *Kumho Tire Co. v. Carmichael*, 526 U.S. 137 (1999), the Supreme Court confirmed that "the general gatekeeping obligation set forth in *Daubert*" "applies when considering all expert testimony, including testimony based on technical and other specialized knowledge." *Clay v. Ford Motor Co.*, 215 F.3d at 667. "It further held that the specific *Daubert* factors – testing, peer review and publication, potential rate of error, and general acceptance in the relevant community – may be considered by the district court even when the proffered expert testimony is not scientific." *Id.* Whether these specific factors are reasonable measures of reliability in a particular case is a matter that the law grants the trial judge broad latitude to determine. *Id.*

"It is the proponent of the testimony that must establish its admissibility by a preponderance of proof." *Nelson v. Tennessee Gas Pipeline Co.*, 243 F.3d 244, 251 (6th Cir. 2001) (citing *Daubert*, 509 U.S. at 592 n.10)).

A district court is not obligated to hold a *Daubert* hearing (*see Clay v. Ford Motor Company*, 215 F.3d at 667; *Nelson*, 243 F.3d at 249) and this Court declines to do so here. A *Daubert* hearing is unnecessary in light of the full briefing of the issues by the parties and the materials submitted to date.

1. The Proposed Expert Testimony Is Relevant

Here, Defendants do not appear to dispute that Hess's proposed testimony is relevant. And even if they did, the Court concludes that his testimony is relevant.

"Evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action." Fed. R. Civ. P. 401.

The proposed expert testimony is that, during the relevant times during which certain robberies occurred, call activity from Defendants' cell phones place them in the general area of the stores where the robberies took place. Such testimony is relevant because it makes a fact of consequence in determining the action (whether Defendants were physically present near the stores on the dates and times of the robberies) more probable than it would be without the evidence. Accordingly, the Court finds that Special Agent Hess's specialized knowledge will help the trier of fact to understand the evidence and to determine a fact in issue in this case. At trial, however, a proper foundation will have to be established regarding the cell phones at issue before Special Agent Hess can testify.

2. The Proposed Expert Testimony Is Sufficiently Reliable.

The Government's Brief indicates that Special Agent Hess has testified as an expert in cell site analysis in over 25 criminal trials, including four cases in this district. Indeed, Special Agent Hess

recently testified as an expert witness in another criminal trial before this Court, *United States v. Reynolds*. *See United States v. Reynolds*, 2013 WL 2480684 (E.D. Mich. June 10, 2013).

In *Reynolds*, the defendant did not argue that Special Agent Hess is not qualified as an expert in the area of cell site analysis. Rather, he argued that cell site analysis should not be permitted because it is not sufficiently reliable because: 1) the testimony is based upon an unreliable methodology for the purpose for which it is offered; and 2) historical cell site analysis is inadmissible to establish a specific location. Both of those arguments were premised on the assumption that the Government was going to have Special Agent Hess testify using cell site analysis to opine that Defendant was present at a *specific location* on the relevant dates and times.

In this case, the Government only seeks to have Hess testify that Defendants' cell phones were in geographic areas "consistent with" the locations where the robberies occurred.

Testimony about cellular phone technology and the ability to determine the general area where calls are placed and received has been widely accepted by federal courts. *See e.g.*, *United States v. Weathers*, 169 F.3d 336, 339 (6th Cir. 1999); *United States v. Schaffer*, 439 Fed. App'x 344, 347 (5th Cir. 2011); *United States v. Jones*,___F.2d___, 2013 WL 246615 (D.D.C. 2013); *United States v. Benford*, 2010 WL 2346305 (N.D. Ind. 2010); *United States v. Allums*, 2009 WL 806748 (D. Utah 2009). This Court again concludes that Special Agent Hess's proposed testimony is the product of reliable principles and methods and he has reliably applied those principles

and methods to the facts of this case.

Moreover, Defense Counsel have indicated that Defendants may call their own expert witness, to challenge the opinions of Special Agent Hess and provide opinion testimony regarding the locations of the cell phones at issue during the relevant time periods.

The weight to be afforded any expert witness testimony presented at trial can be determined by the jury.

The Court shall therefore deny without prejudice Defendants' motion seeking to preclude the expert testimony of Special Agent Hess and shall rule that although Special Agent Hess's proposed testimony regarding cell site analysis is both relevant and reliable, that the Government must lay an appropriate foundation before Special Agent Hess may testify at trial.

CONCLUSION & ORDER

For the reasons set forth above, IT IS ORDERED that Defendants' Motion seeking to Suppress Cell Phone Data (D.E. Nos. 196 & 214) IS DENIED.

IT IS FURTHER ORDERED that the Court DENIES WITHOUT PREJUDICE Defendants' motion seeking to preclude the expert testimony of Special Agent Hess (D.E. Nos. 211 and 215) and RULES that although Special Agent Hess's proposed testimony regarding cell site analysis is both relevant and reliable, the Government must lay an appropriate foundation before Special Agent Hess may testify at trial.

IT IS SO ORDERED.

S/Sean F. Cox

Sean F. Cox

United States District Judge

Dated: December 6, 2013

I hereby certify that a copy of the foregoing document was served upon counsel of record on December 6, 2013, by electronic and/or ordinary mail.

S/Jennifer McCoy

Case Manager

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR AN ORDER FOR DISCLOSURE OF TELECOMMUNICATIONS RECORDS /

Case: 2:11-us-60044A
Judge: Murphy Stephen J.
PEN: Sealed Matter (jj)

APPLICATION

NOW COMES the United States of America, by and through its attorneys, Barbara L. McQuade, United States Attorney, and John N. O'Brien, Assistant United States Attorney, and pursuant to Title 18 United States Code, Section 2703(c) and (d), requests that this Honorable Court issue an Order requiring that:

Adelphia Communications, Adelphia Long Distance, Airlink Wireless, Airvoice Wireless, Allegiance Telecom of California, Inc., AllTel Communications, Alltel Georgia Communications Corp, AllTel Telephone Services, American Cellular, American Paging, Ameritech Michigan, Arch Communications, Arch Paging Communications, Arch Wireless; Astound, AT&T Broadband, AT&T Local Service, AT&T Long Distance, AT&T Wireless Services, Bay Star Communications, Bell South Telecommunications, Bittell Communications, Bluegrass Cellular, Bullseye Telecom, Cavalier Business

Communications, Comcast Cable Communications, CCT Telecom, Cellco Partnership doing business as Verizon Wireless, Cellnet Communications, Cellular Information Systems of Florence, Cellular One, Cellular South, CellulPage, Central Telephone Company of Nevada doing business as Sprint of Nevada, Central Wireless Partnership doing business as Sprint PCS, Cincinnati Bell, Cingular Wireless, Comm South Companies, Commonwealth Communications, Competitive Communications, Inc., Comstat Mobile, Corecomm Limited Cox Communications, Cox Communications Arizona, Dobson Cellular, Crickett Communications, Inc., Cue Paging, DBS Communications, Dobson Communications, Duo County Telephone, Easton Telecomm Service; Edge Wireless LLC, Electric Lightwave, Embarq, Encompass Communications, Ernest Communications, Evans Telephone Company, Excel Communications, Excel Telecommunications, Focal Communications Corporation, Frontier: A Citizens Communications Company, Genesis Communications International, Global Crossing, GTE Paging, Granite Telecommunications, Hartington Telecommunications, Highland Telephone Co-op, ICG Communications, ICG Telecom Group, Iridium North America, ITC Deltacom, IXC Communications, J.D. Services, KMC Telecom, Leap Wireless, Level 3 Communications, Inc., Long Distance Management, Long Distance of Michigan, MCI-Worldcom, MCI-Worldcom Wireless, Metrocall, Metro PCS, M Power Communications, Nationwide Paging, Navigator

Telecommunications LLC, Network Telephone, Networkservices L.L.C., NII Communications, Inc., NSC Communications, O1 Communications, OCI Communications, Omega Services, LLC, One Communications, One Star Long Distance, Optel Texas, Inc. Pac West Telecommunications Incorporated, Pacific Bell, Paetec, Page Plus Communications, Pagemart, Phonetec, Qwest Communications, RCN Communications, Revol, Roseville Telephone Company, Sage Telecom, SBC Ameritech, SBC California, SBC Communications, SBC Nevada Bell, SBC Pacific Bell, SBC Southwestern Bell, Seren Innovations, SkyTel Nationwide, Source One Wireless, Southwestern Bell, Southwestern Bell Wireless, Sprint-Nextel Corporation, Sprint Communications, Sprint Long Distance, Sprint Spectrum L.P., TCG America, Inc., TDS Metrocom, Inc., Telenet Worldwide, Telepacific Communications, Telescape Communications, Teligent, Time-Warner Cable, Time-Warner Telecom, Tracfone Wireless, Inc., Transtel, Trinsic Communications, T-Mobile USA Inc., T-Mobile/Omnipoint, US Cellular, US TelePacific Corp doing business as TelePacific Communications, Variatee Wireless, Verizon California, Verizon District of Columbia, Verizon Maryland, Verizon New England, Verizon New Jersey, Verizon New York, Verizon Northwest, Verizon Texas, Verizon Wireless, Verizon Wireless Paging, Weblink Wireless, Virgin Mobile, VoiceStream Wireless, West Coast PCS LLC doing business as Sure West Wireless, Western Wireless Corporation, Wide Open West, Winstar Communications, WorldCom,

XO Communications, Xspedius Communications
(hereinafter the **telecommunication carriers**)

disclose and furnish the Federal Bureau of Investigation the transactional records described below which pertain to the following telephone numbers, hereafter referred to as "target telephones":

(313) 579-8503
T-Mobile

(313) 412-6845
(313) 424-9573
Metro PCS

(313) 622-0775
(313) 218-2477
(313) 695-9294
Sprint PCS

The transactional records requested include:

A. All subscriber information and toll records including listed and unlisted numbers dialed or otherwise transmitted to and from target telephones from December 1, 2010 to present. In addition, the listed providers are requested to disclose cell site information for the target telephones at call origination and at call termination for incoming and outgoing calls, upon oral or written request by agents of the Federal Bureau of Investigation

B. Records, credit and billing records, can be reached numbers (CBR), custom calling features, and primary long distance carrier, and caller ID for the target telephones.

In support of this application, John N. O'Brien, Assistant United States Attorney states the following:

A. Applicant is an attorney for the government as defined in Rule 1(b)(1)(B) of the Federal Rules of Criminal Procedure and therefore, pursuant to Section 2703(c)(l) and 2703(d) of Title 18, United States Code, may apply for disclosure of telecommunications records.

B. Applicant certifies that based on information from Special Agent Vincente Ruiz of the Federal Bureau of Investigation there exists reasonable grounds to believe that the subscriber information and cell site information requested will be relevant and material to an ongoing criminal investigation. The facts supporting this conclusion include the following:

On April 6, 2011, officers from the Detroit Police Department arrested four individuals, believed to be involved in a series of armed robberies of Radio Shack and T-Mobile stores in Detroit, Michigan.

On April 26, 2011, a cooperating defendant was interviewed about his involvement in those armed robberies and admitted he had a role in eight different robberies that started in December of 2010 and lasted through March of 2011 at Radio Shack and T-Mobile stores in Michigan and Ohio. The defendant further admitted that others involved with the armed robberies were not taken into custody when he was arrested. The core members were usually the same three individuals, but they regularly brought in others to assist as getaway

drivers and look-outs. The defendant identified 15 other individuals who had been involved in at least one of the eight robberies. Four of those individuals had been involved in multiple armed robberies and one had been involved in at least six of the robberies. The defendant also stated that some of the individuals not in custody had been planning to rob more stores in Dayton, Ohio.

It is anticipated that the requested records will assist in identifying and locating the other individuals believed to be involved in the armed robberies.

Additionally, the requested telecommunications records should yield information that is relevant and material to corroborate surveillance information and may identify potential witnesses and/or targets. The requested information will therefore further the Federal Bureau of Investigation in their investigation and provide evidence that Timothy Sanders, Timothy Carpenter and other known and unknown individuals are violating provisions of Title 18, United States Code, §1951.

Applicant requests that the Court issue an Order pursuant to Title 18, United States Code, Section 2703(d) directing the **telecommunication carriers** to provide the requested records to agents of the Federal Bureau of Investigation

Applicant further requests that this application and Order be sealed by the Court until such time as the Court directs otherwise, since disclosure at this time would seriously jeopardize the investigation, and that the Court order the **telecommunication carriers** their agents and

employees not to disclose the existence of this Order or of this investigation to the subscriber, or to any other person unless otherwise directed by the Court.

Applicant further requests that this Court's Order apply not only to the telephone numbers listed above for the target telephone numbers, but also to any changed telephone number(s) subsequently assigned to an instrument bearing the same [ESN] [IMSI] [SIM] [IMEI][MSID][MIN] as the target telephone numbers, or any changed [ESN] [IMSI] [SIM] [IMEI] [MSID][MIN] subsequently assigned to the same telephone numbers as the target telephone numbers, or any additional changed telephone number(s) and or [ESN] [IMSI] [SIM] [IMEI] [MSID][MIN] listed to the same subscriber and/or wireless telephone accounts as the target telephone numbers within the period authorized by this Order.

WHEREFORE, it is respectfully requested that the Court grant an Order directing the **telecommunication carriers** to (1) provide the requested records to agents of the Federal Bureau of Investigation; (2) not to disclose the existence of this Order or the investigation to the subscriber or customer or to any unauthorized person unless or until ordered or authorized to do so by the court; and (3) sealing this application and accompanying Order.

Respectfully submitted,

Barbara L. McQuade
United States Attorney

MAY – 2 '06

John N. O'Brien
Assistant U.S. Attorney.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR AN ORDER FOR DISCLOSURE OF TELECOMMUNICATIONS RECORDS	Case: 2:11-us-60044A Judge: Murphy, Stephen J. PEN: Sealed Matter (jj)

ORDER

This matter, having come before the court pursuant to an application under Title 18, United States Code, Section 2703(d) by John N. O'Brien, an attorney for the Government, requesting the production of certain telecommunications records; the court finds that the applicant has certified and demonstrated to the Court that there are reasonable grounds to believe that the information sought is relevant and material to a legitimate law enforcement investigation into possible violations of Title 18, United States Code, §1951.

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d), that

Adelphia Communications, Adelphia Long Distance, Airlink Wireless, Airvoice Wireless, Allegiance Telecom of California, Inc., AllTel Communications, Alltel Georgia Communications Corp, AllTel Telephone Services, American Cellular, American Paging, Ameritech Michigan, Arch Communications, Arch Paging Commun-

ications, Arch Wireless; Astound, AT&T Broadband, AT&T Local Service, AT&T Long Distance, AT&T Wireless Services, Bay Star Communications, Bell South Telecommunications, Bittell Communications, Bluegrass Cellular, Bullseye Telecom, Cavalier Business Communications, Comcast Cable Communications, CCT Telecom, Cellco Partnership doing business as Verizon Wireless, Cellnet Communications, Cellular Information Systems of Florence, Cellular One, Cellular South, CelluPage, Central Telephone Company of Nevada doing business as Sprint of Nevada, Central Wireless Partnership doing business as Sprint PCS, Cincinnati Bell, Cingular Wireless, Comm South Companies, Commonwealth Communications, Competitive Communications, Inc., Comstat Mobile, Corecomm Limited Cox Communications, Cox Communications Arizona, Dobson Cellular, Crickett Communications, Inc., Cue Paging, DBS Communications, Dobson Communications, Duo County Telephone, Easton Telecomm Service; Edge Wireless LLC, Electric Lightwave, Embarq, Encompass Communications, Ernest Communications, Evans Telephone Company, Excel Communications, Excel Telecommunications, Focal Communications Corporation, Frontier: A Citizens Communications Company, Genesis Communications International, Global Crossing, GTE Paging, Granite Telecommunications, Hartington Telecommunications, Highland Telephone Co-op, ICG Communications, ICG Telecom Group, Iridium North America, ITC Deltacom, IXC Communications, J.D. Services,

KMC Telecom, Leap Wireless, Level 3 Communications, Inc., Long Distance Management, Long Distance of Michigan, MCI-Worldcom, MCI-Worldcom Wireless, Metrocall, Metro PCS, M Power Communications, Nationwide Paging, Navigator Telecommunications LLC, Network Telephone, Networkservices L.L.C., NII Communications, Inc., NSC Communications, O1 Communications, OCI Communications, Omega Services, LLC, One Communications, One Star Long Distance, Optel Texas, Inc. Pac West Telecommunications Incorporated, Pacific Bell, Paetec, Page Plus Communications, Pagemart, Phonetec, Qwest Communications, RCN Communications, Revol, Roseville Telephone Company, Sage Telecom, SBC Ameritech, SBC California, SBC Communications, SBC Nevada Bell, SBC Pacific Bell, SBC Southwestern Bell, Seren Innovations, SkyTel Nationwide, Source One Wireless, Southwestern Bell, Southwestern Bell Wireless, Sprint-Nextel Corporation, Sprint Communications, Sprint Long Distance, Sprint Spectrum L.P., TCG America, Inc., TDS Metrocom, Inc., Telenet Worldwide, Telepacific Communications, Telescape Communications, Teligent, Time-Warner Cable, Time-Warner Telecom, Tracfone Wireless, Inc., Transtel, Trinsic Communications, T-Mobile USA Inc., T-Mobile/Omnipoint, US Cellular, US TelePacific Corp doing business as TelePacific Communications, Variatec Wireless, Verizon California, Verizon District of Columbia, Verizon Maryland, Verizon New England, Verizon New Jersey, Verizon New York, Verizon Northwest,

Verizon Texas, Verizon Wireless, Verizon Wireless Paging, Weblink Wireless, Virgin Mobile, VoiceStream Wireless, West Coast PCS LLC doing business as Sure West Wireless, Western Wireless Corporation, Wide Open West, Winstar Communications, WorldCom, XO Communications, Xspedius Communications (hereinafter the **telecommunication carriers**)

disclose and furnish the Federal Bureau of Investigation the transactional records described below which pertain to the following telephone numbers, hereafter referred to as "target telephones":

(313) 579-8503
T-Mobile

(313) 412-6845
(313) 424-9573
Metro PCS

(313) 622-0775
(313) 218-2477
(313) 695-9294
Sprint PCS

The transactional records requested include:

A. All subscriber information and toll records including listed and unlisted numbers dialed or otherwise transmitted to and from target telephones from December 1, 2010 to present.

B. Records, credit and billing records, can be reached numbers (CBR), custom calling features, and primary long distance carrier, and caller ID for the target telephones.

IT IS FURTHER ORDERED pursuant to 18 U.S.C. Section 2703(c)(l)(B) and 2703(d), that the wireless carriers shall provide the locations of cell/site sector (physical addresses) for the target telephones at call origination and at call termination for incoming and outgoing calls during the relevant time period.

IT IS FURTHER ORDERED that this application and Order be sealed by the Court until such time as the Court directs otherwise, since disclosure at this time would seriously jeopardize the investigation; arid the Court orders that the **telecommunication carriers** their agents and employees not to disclose the existence of this Order or of this investigation to the subscriber, or to any other person unless otherwise directed by the Court.

IT IS FURTHER ORDERED that this authorization applies not only to the telephone numbers listed above for the target telephone numbers, but also to any changed telephone number(s) subsequently assigned to an instrument bearing the same [ESN][IMSI][SIM][IMEI][MSID] [MIN] as the target telephone numbers, or any changed [ESN][IMSI][SIM][IMEI][MSID][MIN] subsequently assigned to the same telephone numbers as the target telephone numbers, or any additional changed telephone number(s) and or [ESN][IMSI][SIM][IMEI][MSID][MIN] listed to the same subscriber and/or wireless telephone account as the target telephone numbers within the period authorized by this Order;

IT IS FURTHER ORDERED that the local, long distance and wireless carriers be compensated by the investigative agency for reasonable expenses incurred in providing technical assistance.

Honorable Laurie Michaelson
United States Magistrate Judge

Dated: 5/2/11

A True Copy
U. S. Attorney's Office
Eastern District of Michigan
BY: _____
Paralegal Specialist

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR AN ORDER FOR DISCLOSURE OF TELECOMMUNICATIONS RECORDS /	Tracking No.: 11US60044-C Hon. Stephen J. Murphy, III

APPLICATION

NOW COMES the United States of America, by and through its attorneys, Barbara L. McQuade, United States Attorney, and John N. O'Brien, Assistant United States Attorney, and pursuant to Title 18 United States Code, Section 2703(c) and (d), requests that this Honorable Court issue an Order requiring that:

Adelphia Communications, Adelphia Long Distance, Airlink Wireless, Airvoice Wireless, Allegiance Telecom of California, Inc., AllTel Communications, Alltel Georgia Communications Corp, AllTel Telephone Services, American Cellular, American Paging, Ameritech Michigan, Arch Communications, Arch Paging Communications, Arch Wireless; Astound, AT&T Broadband, AT&T Local Service, AT&T Long Distance, AT&T Wireless Services, Bay Star Communications, Bell South Telecommunications, Bittell Communications, Bluegrass Cellular, Bullseye Telecom, Cavalier Business

Communications, Comcast Cable Communications, CCT Telecom, Cellco Partnership doing business as Verizon Wireless, Cellnet Communications, Cellular Information Systems of Florence, Cellular One, Cellular South, CelluPage, Central Telephone Company of Nevada doing business as Sprint of Nevada, Central Wireless Partnership doing business as Sprint PCS, Cincinnati Bell, Cingular Wireless, Comm South Companies, Commonwealth Communications, Competitive Communications, Inc., Comstat Mobile, Corecomm Limited Cox Communications, Cox Communications Arizona, Dobson Cellular, Crickett Communications, Inc., Cue Paging, DBS Communications, Dobson Communications, Duo County Telephone, Easton Telecomm Service; Edge Wireless LLC, Electric Lightwave, Embarq, Encompass Communications, Ernest Communications, Evans Telephone Company, Excel Communications, Excel Telecommunications, Focal Communications Corporation, Frontier: A Citizens Communications Company, Genesis Communications International, Global Crossing, GTE Paging, Granite Telecommunications, Hartington Telecommunications, Highland Telephone Co-op, ICG Communications, ICG Telecom Group, Iridium North America, ITC Deltacom, IXC Communications, J.D. Services, KMC Telecom, Leap Wireless, Level 3 Communications, Inc., Long Distance Management, Long Distance of Michigan, MCI-Worldcom, MCI- Worldcom Wireless, Metrocall, Metro PCS, M Power Communications, Nationwide Paging, Navigator

Telecommunications LLC, Network Telephone, Networkservices L.L.C., NII Communications, Inc., NSC Communications, O1 Communications, OCI Communications, Omega Services, LLC, One Communications, One Star Long Distance, Optel Texas, Inc. Pac West Telecommunications Incorporated, Pacific Bell, Pactec, Page Plus Communications, Pagemart, Phonetec, Qwest Communications, RCN Communications, Revol, Roseville Telephone Company, Sage Telecom, SBC Ameritech, SBC California, SBCCommunications, SBC Nevada Bell, SBC Pacific Bell, SBC Southwestern Bell, Seren Innovations, SkyTel Nationwide, Source One Wireless, Southwestern Bell, Southwestern Bell Wireless, Sprint-Nextel Corporation, Sprint Communications, Sprint Long Distance, Sprint Spectrum L.P., TCG America, Inc., TDS Metrocom, Inc., Telenet Worldwide, Telepacific Communications, Telescape Communications, Teligent, Time-Warner Cable, Time-Warner Telecom, Tracfone Wireless, Inc., Transtel, Trinsic Communications, T-Mobile USA Inc., T-Mobile/Omnipoint, US Cellular, US TelePacific Corp doing business as TelePacific Communications, Variatee Wireless, Verizon California, Verizon District of Columbia, Verizon Maryland, Verizon New England, Verizon New Jersey, Verizon New York, Verizon Northwest, Verizon Texas, Verizon Wireless, Verizon Wireless Paging, Weblink Wireless, Virgin Mobile, VoiceStream Wireless, West Coast PCS LLC doing business as Sure West Wireless, Western Wireless Corporation, Wide Open West, Winstar Communications, WorldCom,

XO Communications, Xspedius Communications (hereinafter the **telecommunication carriers**)

disclose and furnish the Federal Bureau of Investigation the transactional records described below which pertain to the following telephone numbers, hereafter referred to as "target telephone":

(313) 412-6845
Metro PCS telephone number roaming on Sprint's cellular tower network

The transactional records requested include:

A. All subscriber information and toll records including listed and unlisted numbers dialed or otherwise transmitted to and from target telephones from March 1, 2011 to March 7, 2011, including roaming tower call detail records with cell site information. In addition, the listed providers are requested to disclose cell site information for the target telephone at call origination and at call termination for incoming and outgoing calls, upon oral or written request by agents of the Federal Bureau of Investigation.

B. Records, credit and billing records, can be reached numbers (CBR), custom calling features, and primary long distance carrier, and caller ID for the target telephone.

In support of this application, John N. O'Brien, Assistant United States Attorney states the following:

A. Applicant is an attorney for the government as defined in Rule 1(b)(1)(B) of the Federal Rules of Criminal Procedure and

therefore, pursuant to Section 2703(c)(l) and 2703(d) of Title 18, United States Code, may apply for disclosure of telecommunications records.

B. Applicant certifies that based on information from Special Agent Vincente Ruiz of the Federal Bureau of Investigation there exists reasonable grounds to believe that the subscriber information and cell site information requested will be relevant and material to an ongoing criminal investigation. The facts supporting this conclusion include the following:

On April 6, 2011, officers from the Detroit Police Department arrested four individuals believed to be involved in a series of armed robberies of Radio Shack and T-Mobile stores in Detroit, Michigan.

On April 26, 2011, a cooperating defendant was interviewed about his involvement in those armed robberies and admitted he had a role in nine different robberies that started in December of 2010 and lasted through March of 2011 at Radio Shack and T-Mobile stores in Michigan and Ohio. The defendant further admitted that others involved with the armed robberies were not taken into custody when he was arrested. The core members were usually the same three individuals, but they regularly brought in others to assist as getaway drivers and lookouts. The defendant identified 15 other individuals who had been involved in at least one of the nine robberies. Seven of those individuals had been involved in multiple armed robberies and three had been involved in at least five of the robberies. The defendant also stated that some of the individuals not in custody had been planning to rob more stores in Dayton, Ohio.

The cooperating defendant provided his cellular telephone number and identified numbers of some of the individuals involved. A review of the historical call detail records revealed other numbers that were contacted during and around the times of the robberies.

It is anticipated that the requested records will assist in identifying and locating the other individuals believed to be involved in the armed robberies.

Additionally, the requested telecommunications records should yield information that is relevant and material to corroborate surveillance information and may identify potential witnesses and/or targets. The requested information will therefore further the Federal Bureau of Investigation in their investigation and provide evidence that Timothy Sanders, Timothy Carpenter and other known and unknown individuals are violating provisions of Title 18, United States Code; §1951.

Applicant requests that the Court issue an Order pursuant to Title 18, United States Code, Section 2703(d) directing the **telecommunication carriers** to provide the requested records to agents of the Federal Bureau of Investigation.

Applicant further requests that this application and Order be sealed by the Court until such time as the Court directs otherwise, since disclosure at this time would seriously jeopardize the investigation, and that the Court order the **telecommunication carriers** their agents and employees not to disclose the existence of this Order or of this investigation to the subscriber, or to any

other person unless otherwise directed by the Court.

Applicant further requests that this Court's Order apply not only to the telephone numbers listed above for the target telephone numbers, but also to any changed telephone number(s) subsequently assigned to an instrument bearing the same [ESN][IMSI][SIM][IMEI][MSID][MIN] as the target telephone numbers, or any changed [ESN][IMSI][SIM][IMEI][MSID][MIN] subsequently assigned to the same telephone numbers as the target telephone numbers, or any additional changed telephone number(s) and or [ESN] [IMSI] [SIM] [IMEI][MSID][MIN] listed to the same subscriber and/or wireless telephone accounts as the target telephone numbers within the period authorized by this Order.

WHEREFORE, it is respectfully requested that the Court grant an Order directing the **telecommunication carriers** to (1) provide the requested records to agents of the Federal Bureau of Investigation; (2) not to disclose the existence of this Order or the investigation to the subscriber or customer or to any unauthorized person unless or until ordered or authorized to do so by the court; and (3) sealing this application and accompanying Order.

Respectfully submitted,

Barbara L. McQuade
United States Attorney

John N. O'Brien
Assistant U.S. Attorney

Dated: Jun-7 2011

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR AN ORDER FOR DISCLOSURE OF TELECOMMUNICATIONS RECORDS
_____/

Tracking No.: 11US60044-C
Hon. Stephen J. Murphy, III

ORDER

This matter, having come before the court pursuant to an application under Title 18, United States Code, Section 2703(d) by John N. O'Brien, an attorney for the Government, requesting the production of certain telecommunications records; the court finds that the applicant has certified and demonstrated to the Court that there are reasonable grounds to believe that the information sought is relevant and material to a legitimate law enforcement investigation into possible violations of Title 18, United States Code, §1951.

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d), that

Adelphia Communications, Adelphia Long Distance, Airlink Wireless, Airvoice Wireless, Allegiance Telecom of California, Inc., AllTel Communications, Alltel Georgia Communications Corp, AllTel Telephone Services, American Cellular, American Paging, Ameritech Michigan, Arch Communications, Arch Paging Commun-

ications, Arch Wireless; Astound, AT&T Broadband, AT&T Local Service, AT&T Long Distance, AT&T Wireless Services, Bay Star Communications, Bell South Telecommunications, Bittell Communications, Bluegrass Cellular, Bullseye Telecom, Cavalier Business Communications, Comcast Cable Communications, CCT Telecom, Cellco Partnership doing business as Verizon Wireless, Cellnet Communications, Cellular Information Systems of Florence, Cellular One, Cellular South, CelluPage, Central Telephone Company of Nevada doing business as Sprint of Nevada, Central Wireless Partnership doing business as Sprint PCS, Cincinnati Bell, Cingular Wireless, Comm South Companies, Commonwealth Communications, Competitive Communications, Inc., Comstat Mobile, Corecomm Limited Cox Communications, Cox Communications Arizona, Dobson Cellular, Crickett Communications, Inc., Cue Paging, DBS Communications, Dobson Communications, Duo County Telephone, Easton Telecomm Service; Edge Wireless LLC, Electric Lightwave, Embarq, Encompass Communications, Ernest Communications, Evans Telephone Company, Excel Communications, Excel Telecommunications, Focal Communications Corporation, Frontier: A Citizens Communications Company, Genesis Communications International, Global Crossing, GTE Paging, Granite Telecommunications, Hartington Telecommunications, Highland Telephone Co-op, ICG Communications, ICG Telecom Group, Iridium North America, ITC Deltacom, IXC Communications, J.D. Services,

KMC Telecom, Leap Wireless, Level 3 Communications, Inc., Long Distance Management, Long Distance of Michigan, MCI-Worldcom, MCI- Worldcom Wireless, Metrocall, Metro PCS, M Power Communications, Nationwide Paging, Navigator Telecommunications LLC, Network Telephone, Networkservices L.L.C., NII Communications, Inc., NSC Communications, O1 Communications, OCI Communications, Omega Services, LLC, One Communications, One Star Long Distance, Optel Texas, Inc. Pac West Telecommunications Incorporated, Pacific Bell, Pactec, Page Plus Communications, Pagemart, Phonetec, Qwest Communications, RCN Communications, Revol, Roseville Telephone Company, Sage Telecom, SBC Ameritech, SBC California, SBCCommunications, SBC Nevada Bell, SBC Pacific Bell, SBC Southwestern Bell. Seren Innovations, SkyTel Nationwide, Source One Wireless, Southwestern Bell, Southwestern Bell Wireless, Sprint-Nextel Corporation, Sprint Communications, Sprint Long Distance, Sprint Spectrum L.P., TCG America, Inc., TDS Metrocom, Inc., Telenet Worldwide, Telepacific Communications, Telescape Communications, Teligent, Time-Warner Cable, Time-Warner Telecom, Tracfone Wireless, Inc., Transtel, Trinsic Communications, T-Mobile USA Inc., T-Mobile/Omnipoint, US Cellular, US TelePacific Corp doing business as TelePacific Communications, Variatee Wireless, Verizon California, Verizon District of Columbia, Verizon Maryland, Verizon New England, Verizon New Jersey, Verizon New York, Verizon Northwest,

Verizon Texas, Verizon Wireless, Verizon Wireless Paging, Weblink Wireless, Virgin Mobile, VoiceStream Wireless, West Coast PCS LLC doing business as Sure West Wireless, Western Wireless Corporation, Wide Open West, Winstar Communications, WorldCom, XO Communications, Xspedius Communications (hereinafter the **telecommunication carriers**)

disclose and furnish the Federal Bureau of Investigation the transactional records described below which pertain to the following telephone numbers, hereafter referred to as "target telephones":

(313) 412-6845
Metro PCS telephone number roaming on Sprint's cellular tower network

The transactional records requested include:

A. All subscriber information and toll records including listed and unlisted numbers dialed or otherwise transmitted to and from target telephone from March 1, 2011 to March 7, 2011.

B. Records, credit and billing records, can be reached numbers (CBR), custom calling features, and primary long distance carrier, and caller ID for the target telephones.

IT IS FURTHER ORDERED pursuant to 18 U.S.C. Section 2703(c)(l)(B) and 2703(d), that the wireless carriers shall provide the locations of cell/site sector (physical addresses) for the target telephones at call origination and at call termination for incoming and outgoing calls during the relevant time period.

IT IS FURTHER ORDERED that this application and Order be sealed by the Court until such time as the Court directs otherwise, since disclosure at this time would seriously jeopardize the investigation; and the Court orders that the telecommunication carriers their agents and employees not to disclose the existence of this Order or of this investigation to the subscriber, or to any other person unless otherwise directed by the Court.

IT IS FURTHER ORDERED that this authorization applies not only to the telephone numbers listed above for the target telephone numbers, but also to any changed telephone number(s) subsequently assigned to an instrument bearing the same [ESN][IMSI][SIM][IMEI][MSID][MIN] as the target telephone numbers, or any changed [ESN][IMSI][SIM][IMEI][MSID][MIN] subsequently assigned to the same telephone numbers as the target telephone numbers, or any additional changed telephone number(s) and or [ESN][IMSI][SIM][IMEI][MSID][MIN] listed to the same subscriber and/or wireless telephone account as the target telephone numbers within the period authorized by this Order;

IT IS FURTHER ORDERED that the local, long distance and wireless carriers be compensated by the investigative agency for reasonable expenses incurred in providing technical assistance.

A True Copy
U. S. Attorney's Office
Eastern District of Michigan
By _____
Foreign Specialist

Honorable Mark A. Randon
United States Magistrate Judge

Dated: 6/7/11

FEDERAL BUREAU OF INVESTIGATION
CELLULAR ANALYSIS SURVEY TEAM

Cellular Analysis

(313) 579-8507
(313) 412-6845

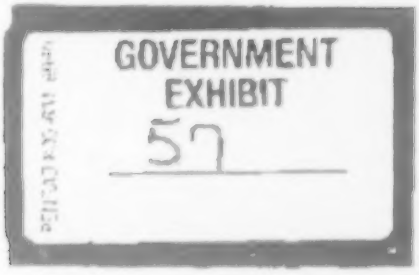
SA Christopher J. Hess

Detroit Division

Detroit Major Crimes Task Force

281R-DE-105923

November 5, 2013



INVESTIGATIVE INFORMATION

CASE FACTS: Special Agent Vicente Ruiz, Federal Bureau of Investigation, Detroit Division, investigated a case involving multiple armed robberies dating back to 2010. The robberies occurred in the Detroit metropolitan area as well as Warren, Ohio. Investigators linked cellular telephone number (313) 579-8507 to Timothy Sanders (Target Cell Phone 1) and (313) 412-6845 to Timothy Carpenter (Target Telephone 2).

REQUESTING INFORMATION

PURPOSE OF ANALYSIS: SA Ruiz requested cell site analysis of the target phones to determine the geographic area where the target phones were located in relation to incident date(s) and time(s).

TARGET CELL PHONE 1 INFORMATION

SERVICE PROVIDER: T-Mobile

SUBSCRIBER INFORMATION: N/A

TYPE OF RECORDS BEING ANALYZED: Call Detail Records (CDRs)

SOURCE FROM WHICH RECORDS ACQUIRED: SA Vicente Ruiz furnished an electronic copy of records associated with Target Phone 1.

DATE & TIME RANGE USED FOR ANAYLSIS:

03/04/2011, 2:52 p.m.

TARGET CELL PHONE 2 INFORMATION

SERVICE PROVIDER: Metro PCS

SUBSCRIBER INFORMATION: Michael Mayers

TYPE OF RECORDS BEING ANALYZED: Call Detail Records (CDRs)

SOURCE FROM WHICH RECORDS ACQUIRED: SA Vicente Ruiz furnished an electronic copy of records associated with Target Phone 2.

DATE & TIME RANGE USED FOR ANAYLSIS:

12/13/2010, 10:35 a.m.

12/18/2010, 4:50 p.m.

03/04/2011, 2:52 p.m.

04/05/2011, 2:40 p.m.

BASIC PRINCIPALS UTILIZED IN RECORD ANALYSIS

TECHNOLOGY

Cell phones are RADIOS that use RADIO FREQUENCIES to communicate. Some additional facts:

- Cell phones (when "on") constantly scan their environment looking for the best signal from the tower.

- The best signal generally comes from the

tower that is CLOSEST to the phone, or in its direct LINE OF SIGHT.

- The tower with the best signal is the one the handset will use for service, this is the serving cell and will be used to make and receive calls

- The phone will use the serving cell to make/receive calls.

- The phone "sees" other towers around the SERVING CELL and will constantly measure those signal strengths. However the phone will not randomly reselect to an adjacent tower unless the tower is on its "neighbor list" which is controlled by the network service provider. This allows the network to accurately manage and control the subscribers.

- As the phone moves, it will choose a new serving cell based on signal strength and neighbor list. If this occurs while the phone is in a call, the phone will "handoff" the call to the next cell site/sector. Therefore some service providers, such as SPRINT and AT&T, show a "beginning cell site" (call originated) and an "ending cell site" (call ended) in their records.

CELL SITES AND SECTORS

Cell towers (also known as CELL SITES or BASE TRANSCEIVER STATIONS) come in all shapes and sizes and can be located anywhere (church steeples, water towers, sides of buildings, etc.).

- A typical cell tower has THREE, 120° sectors. The service provider sometimes labels the sectors numerically, such as 1, 2, 3, or ALPHA, BETA, GAMMA. Sector 1 (or Alpha) typically covers the NORTHERN sector of the tower, 2 (EAST), 3 (WEST).

- It is important to note that each BTS has its own unique identifier, this identifier is used to track which towers the handsets use and is like a fingerprint on the network. It is not duplicated anywhere else.

- The location of a cell tower is often determined by sales/ marketing, capacity, improvement of coverage, or expansion/growth of a service provider. Generally there are more towers with overlapping coverage in urban areas; less towers (less coverage) in rural areas.

- Antennas on cell towers have downward tilt and are pointed towards the earth. The antenna arrays are fine tuned to provide a specific area of coverage. As RF travels away from the tower, their strength (and distance) diminishes. A good illustration of this principle is to think of a cell tower and the area that it covers as an upside down funnel.

Cellular Phone Record Analysis of (313) 579-8507

Date Range: 03/04/2011, 2:52 p.m.

ANALYSI S (313) 579-8507 (Target Telephone 1)

A review of the Call Detail Records (CDRs) revealed that there was call activity during the period covered by the records. The analysis was focused on the specific date and time referenced above. The CDRs contained the cell sites associated with each call event. The cell sites identified on the call detail records were compared to T-Mobile tower records. The tower records were imported to Microsoft MapPoint to visually depict the locations of towers within the T-Mobile network in the Detroit and Ohio markets. The cell sites identified on the CDRs were then plotted utilizing the corresponding tower records.

As a result, during the specified date, cell sites that were utilized by Target Telephone 1 were concentrated within the Warren, Ohio area. Analysis of the specified time period yielded the following results:

> 03/04/ 2011: A call was initiated at 2:20 PM. The duration of the call activity was over 31 minutes. The call originated and terminated on cell site 8499 5703 located in the geographic area consistent with the robbery scene at 2553 Parkman, Warren, Ohio.

A representation of this analysis can be seen in the attached Microsoft PowerPoint presentation labeled Attachment A.

Cellular Phone Record Analysis of (313) 412-6845

Date Range: 12/13/2010, 10:35 a.m.; 12/18/2010, 4:50 p.m.; 03/04/2011, 2:52 p.m.; 04/05/ 2011, 2:40 p.m.

ANALYSIS (313) 412-6845 (Target Telephone 2)

A review of the Call Detail Records (CDRs) revealed that there was call activity during the period covered by the records. The analysis was focused on the specific dates and times referenced above. The CDRs contained the cell sites associated with each call event. The cell sites identified on the call detail records were compared to the tower records furnished by Metro PCS. The tower records were imported to Microsoft MapPoint to visually depict the locations of towers within the Metro PCS network in the Detroit Metropolitan Area. On 03/04/2011, Target Telephone 2 was located outside of the Metro PCS market and roaming on the Sprint PCS network in Ohio. Sprint PCS tower records in the Ohio market were imported to Microsoft MapPoint as well. The cell sites identified on the CDRs were then plotted utilizing the corresponding tower records.

As a result, cell sites that were utilized by Target Telephone 2 were in the Detroit, Michigan and Warren, Ohio. On Analysis of the specified time periods yielded the following results:

> 12/13/2010, 10:35 a.m.: Call activity immediately prior to the reported time of the robbery utilized tower 127, sector 1 and sector 2. The tower is located

southwest of the robbery scene. The next call originated on an adjacent tower north of the robbery scene.

12/18/2010, 4:50 p.m.: Call activity in and around the time of the robbery incident utilized tower 173 and tower 188. The towers are located south of the robbery scene.

03/04/2011, 2:52 p.m.: Call activity before and after the robbery utilized tower 208 293 on the Sprint network. The tower is located south of the robbery location.

04/05/2011, 2:40 p.m.: Call activity prior to the robbery incident utilized tower 502 and tower 170. Tower 502 is located south of the robbery scene.

A representation of this analysis can be seen in the attached Microsoft PowerPoint presentation labeled Attachment B.

CONCLUSION

LOCATION OF TARGET CELL PHONE: Based upon my training, experience, and analysis, it is determined that:

Target Telephone 1 utilized cell sites in the geographic area consistent with the robbery scene located at 2553 Parkman, Warren, Ohio on March 4, 2011.

Target Telephone 2 utilized cell sites in the geographic area consistent with the robbery scenes on December 13 and 18, 2010, as well as March 4, 2011, and April 5, 2011.

ATTACHMENT A

Target Number (313) 579-8507

March 4, 2011, 2:52 p.m.

- Call activity was initiated at 14:20 (2:20 p.m.) lasting over 31 minutes.
- The activity originated and terminated on cell site 8496 5703.

ATTACHMENT B

Target Number (313) 412-6845
December 13, 2010, 10:35 a.m.

Target Number (313) 412-6845
December 18, 2010, 4:50 p.m.

Target Number (313) 412-6845
March 4, 2011, 2:52 p.m.
Metro PCS
Sprint PCS

Target Number (313) 412-6845

April 5, 2011, 2:40 p.m.

ECORD
AND
BRIEF

FILED
JAN 27 2017
OFFICE OF THE CLERK
SUPREME COURT, U.S.

No. 16-402

In the Supreme Court of the United States

TIMOTHY IVORY CARPENTER, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

NOEL J. FRANCISCO
Acting Solicitor General
Counsel of Record
KENNETH A. BLANCO
Acting Assistant Attorney General
JENNY C. ELLICKSON
Attorney
Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

QUESTION PRESENTED

Whether the government's acquisition, pursuant to a court order issued under 18 U.S.C. 2703(d), of historical cell-site records created and maintained by a cellular-service provider violates the Fourth Amendment rights of the individual customer to whom the records pertain.

TABLE OF CONTENTS

Page

Opinions below 1
Jurisdiction 1
Statement 1
Argument 10
Conclusion 32

TABLE OF AUTHORITIES

Cases:

Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, In re, 620 F.3d 304 (3d Cir. 2010) 26, 27, 28
Application of the U.S. for Historical Cell Site Data, In re, 724 F.3d 600 (5th Cir. 2013) 15, 26
Commonwealth v. *Augustine*, 4 N.E.3d 846 (Mass. 2014) 29
Davis v. *United States*, 131 S. Ct. 2419 (2011) 31
Davis v. *United States*, 136 S. Ct. 479 (2015) 10
Donaldson v. *United States*, 400 U.S. 517 (1971) 18
Ferguson v. *City of Charleston*, 532 U.S. 67 (2001) 22
Guerrero v. *United States*, 135 S. Ct. 1548 (2015) 10
Illinois v. *Krull*, 480 U.S. 340 (1987) 30
Katz v. *United States*, 389 U.S. 347 (1967) 11
Kyllo v. *United States*, 533 U.S. 27 (2001) 11, 17, 18
Maryland v. *King*, 133 S. Ct. 1958 (2013) 23, 25, 26
Neder v. *United States*, 527 U.S. 1 (1999) 31
Oklahoma Press Publ'g Co. v. *Walling*, 327 U.S. 186 (1946) 11, 23, 24
Reporters Comm. for Freedom of the Press v. *American Tel. & Tel. Co.*, 593 F.2d 1030 (D.C. Cir. 1978), cert. denied, 440 U.S. 949 (1979) 28

Cases—Continued: Page

Riley v. *California*, 134 S. Ct. 2473 (2014) 19, 20, 22
Smith v. *Maryland*, 442 U.S. 735 (1979) ..... *passim*
State v. *Earls*, 70 A.3d 630 (N.J. 2013) 29
Tracey v. *State*, 152 So. 3d 504 (Fla. 2014) 29
United States v. *Davis*, 785 F.3d 498 (11th Cir.), cert. denied, 136 S. Ct. 479 (2015) 15, 24, 25, 26
United States v. *Graham*, 824 F.3d 421 (4th Cir.), petitions for cert. pending, No. 16-6308 (filed Sept. 26, 2016), and No. 16-6694 (filed Oct. 27, 2016) 16, 17, 26
United States v. *Jones*, 132 S. Ct. 945 (2012) ..... *passim*
United States v. *Karo*, 468 U.S. 705 (1984) 17
United States v. *Knotts*, 460 U.S. 276 (1983) 20
United States v. *Leon*, 468 U.S. 897 (1984) 30
United States v. *Maynard*, 615 F.3d 544 (D.C. Cir. 2010), aff'd on other grounds *sub nom. United States* v. *Jones*, 132 S. Ct. 945 (2012) 28
United States v. *Miller*, 425 U.S. 435 (1976) ..... *passim*
United States v. *Salerno*, 481 U.S. 739 (1987) 25
United States v. *Watson*, 423 U.S. 411 (1976) 23
Vernonia Sch. Dist. 47J v. *Acton*, 515 U.S. 646 (1995) 23
Zanders v. *State*, 58 N.E.3d 254 (Ind. Ct. App.), vacated and transfer granted, 62 N.E.3d 1202 (Ind. 2016) 28

Constitution and statutes:

U.S. Const. Amend. IV ..... *passim*
Bank Secrecy Act, 12 U.S.C. 1829b(d) 3, 5, 12
Hobbs Act, 18 U.S.C. 1951(a) 2, 5

Statutes—Continued: Page

Stored Communications Act, 18 U.S.C. 2701 *et seq.* 2
18 U.S.C. 2702(a) 3
18 U.S.C. 2703 3
18 U.S.C. 2703(c)(1)(A) 3, 27
18 U.S.C. 2703(c)(1)(B) 3
18 U.S.C. 2703(c)(2)(A)-(C) 3
18 U.S.C. 2703(d) 3, 9, 24, 25
18 U.S.C. 2711(1) 3
18 U.S.C. 924(c) 2, 5
18 U.S.C. 2510(1) 3

In the Supreme Court of the United States

No. 16-402

TIMOTHY IVORY CARPENTER, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

OPINIONS BELOW

The opinion of the court of appeals (Pet. App. 1a-32a) is reported at 819 F.3d 880. The opinion of the district court denying petitioner's motion to suppress (Pet. App. 34a-48a) is not published in the Federal Supplement but is available at 2013 WL 6385838.

JURISDICTION

The judgment of the court of appeals was entered on April 13, 2016. A petition for rehearing was denied on June 29, 2016 (Pet. App. 33a). The petition for a writ of certiorari was filed on September 26, 2016. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

STATEMENT

Following a jury trial in the United States District Court for the Eastern District of Michigan, petitioner was convicted on six counts of aiding and abetting

Hobbs Act robbery, in violation of 18 U.S.C. 1951(a), and five counts of aiding and abetting the use or carrying of a firearm during and in relation to a crime of violence, in violation of 18 U.S.C. 924(c). Pet. App. 5a-6a. The district court sentenced petitioner to 1395 months in prison. *Id.* at 7a. The court of appeals affirmed. *Id.* at 1a-24a.

1. Between December 2010 and December 2012, petitioner and his co-conspirators committed a string of armed robberies at Radio Shack and T-Mobile stores in Ohio and Michigan. Pet. App. 3a, 6a; Presentence Investigation Report (PSR) ¶¶ 16-23. Petitioner organized most of the robberies, often supplied the guns, and typically acted as a lookout during the robberies. Pet. App. 5a. On petitioner's signal, a group of robbers "entered the store, brandished their guns, herded customers and employees to the back, and ordered the employees to fill the robbers' bags with new smartphones." *Ibid.* After each robbery, the team disposed of the guns and getaway vehicle and sold the stolen merchandise. *Ibid.*; PSR ¶¶ 17-23.

2. a. In April 2011, police arrested four of petitioner's co-conspirators, and one of them confessed that the group had robbed nine stores in Michigan and Ohio between December 2010 and March 2011. Pet. App. 3a. The robber who confessed to the crimes gave the Federal Bureau of Investigation (FBI) his cellular telephone number and the cell-phone numbers of other co-conspirators. *Ibid.* The FBI reviewed his call records and identified additional numbers he had called around the time of the robberies. *Ibid.*

In May and June 2011, the government applied to federal magistrate judges for three court orders pursuant to the Stored Communications Act (SCA),

18 U.S.C. 2701 *et seq.* See Pet. App. 3a, 49a-55a, 62a-68a; Gov't C.A. Br. 9. Those applications sought orders directing certain cellular-service providers, including MetroPCS and Sprint, to disclose specified records for 16 telephone numbers, including a cellphone number that petitioner was known to use. Pet. App. 3a-4a, 49a-55a, 62a-68a; Gov't C.A. Br. 9.

The SCA generally prohibits communications providers from disclosing certain records pertaining to their subscribers to a governmental entity, but permits the government to acquire such records in certain circumstances. 18 U.S.C. 2510(1), 2702(a), 2703, 2711(1). As relevant here, the government may obtain "a record or other information pertaining to a subscriber * * * (not including the contents of communications)" either through a warrant or through "a court order for such disclosure under [18 U.S.C. 2703(d)]." 18 U.S.C. 2703(c)(1)(A) and (B). To obtain a court order, the government must "offer[] specific and articulable facts showing that there are reasonable grounds to believe that * * * the records or other information sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. 2703(d). The records that the government may obtain under such an order include a subscriber's name and address, "telephone connection records," and "records of session times and durations." 18 U.S.C. 2703(c)(2)(A)-(C).

The records that the government sought for petitioner's cell phone included "[a]ll subscriber information, toll records and call detail records including listed and unlisted numbers dialed or otherwise transmitted to and from [petitioner's] telephone[]." Pet. App. 4a (first set of brackets in original). The government also sought records known as historical

"cell-site" records, which show which cell towers a cell phone has connected with while in use. *Id.* at 4a-5a. Cellular-service providers create and retain cell-site records in the ordinary course of business for their own purposes, including to find weak spots in their cellular networks and to determine whether to charge customers roaming charges for particular calls. *Id.* at 5a, 7a, 10a.

In this case, the government sought "cell site information for [petitioner's] telephone[] at call origination and at call termination for incoming and outgoing calls." Pet. App. 4a. As an FBI expert testified, "cellphones work by establishing a radio connection with nearby cell towers (or 'cell sites')." *Id.* at 5a. "[I]ndividual towers project different signals in each direction or 'sector,'" with three or six sectors per tower, "so that a cellphone located on the north side of a cell tower will use a different signal than a cellphone located on the south side of the same tower." *Ibid.*; see *id.* at 14a. In an urban area like Detroit, the FBI expert explained, "each cell site covers 'typically anywhere from a half-mile to two miles.'" *Id.* at 5a. By requesting "historical" cell-site records, the government sought data pertaining only to past calls and did not seek to monitor the connections of petitioner's phone to cell towers in real time.

The magistrate judges granted the government's applications and issued the requested orders. Pet. App. 56a-61a, 69a-73a. Petitioner's wireless carrier, MetroPCS, then produced 127 days of historical cell-site records for petitioner's phone number, which MetroPCS had made in the ordinary course of business for billing and other business purposes. *Id.* at 7a, 10a; see Pet. 5 & n.2. In addition, Sprint produced

seven days of historical cell-site records for petitioner's phone number for early March 2011, when petitioner's cell phone was connecting to Sprint cellular towers in Warren, Ohio, pursuant to a roaming agreement between MetroPCS and Sprint. 12/13/13 Tr. (Tr.) 58-60; Pet. App. 88a; see Pet. 5.

From the historical cell-site records as well as MetroPCS and Sprint records identifying the locations of their towers, the government was able to infer the approximate location of petitioner's phone at the time it made and received calls. Pet. App. 6a; Tr. 93-94.[1] Because the cell-site records "could do no better than locate [petitioner's] cellphone[] within a 120- (or sometimes 60-) degree wedge extending between one-half mile and two miles in length," however, the government could determine the location of petitioner's phone only "within a 3.5 million square-foot to 100 million square-foot area." Pet. App. 14a. The government ultimately determined that petitioner's cell phone communicated with cell towers in the general vicinity of the sites of four robberies between December 2010 and April 2011. *Id.* at 6a.

b. Petitioner was indicted on six counts of aiding and abetting Hobbs Act robbery, in violation of 18 U.S.C. 1951(a), and six counts of aiding and abetting the use or carrying of a firearm during and in relation to a federal crime of violence, in violation of 18 U.S.C. 924(c). Pet. App. 4a; D. Ct. Doc. 119 (June 18, 2013). Before trial, petitioner moved to suppress the historical cell-site records, alleging that the government had obtained them from MetroPCS and Sprint in violation

---

[1] The records did not contain any cell-site information for text messages or for times when petitioner's cell phone was turned on but was not making or receiving a call. See Pet. App. 7a.

of the Fourth Amendment. Pet. App. 7a-8a. Petitioner argued that MetroPCS's and Sprint's production of their business records constituted a search of petitioner that could be conducted only pursuant to a search warrant supported by probable cause. *Ibid.*

The district court denied the motion to suppress. Pet. App. 34a-48a. The court observed that petitioner had "not directed the Court to a single decision by any United States Court of Appeals * * * that supports [his] position," and it concluded that "there is no legitimate expectation of privacy in cell site data." *Id.* at 38a. The district court ruled in the alternative that, even if a warrant were required to obtain historical cell-site data, "the evidence should not be suppressed * * * because the agents relied in good faith on the [SCA] in obtaining the evidence." *Id.* at 38a n.1.

c. The case proceeded to trial, where seven of petitioner's accomplices testified about petitioner's involvement in the robberies. Pet. App. 5a. The witnesses described how petitioner "organized most of the robberies and often supplied the guns." *Ibid.* The government also introduced videotapes and eyewitness testimony placing petitioner near the relevant robbery scenes. See Gov't C.A. Br. 45-47 (describing evidence). In addition, an FBI agent offered expert testimony about the cell-site data for petitioner's phone. Pet. App. 5a-6a. The agent presented maps showing that petitioner's phone was within a half-mile to two miles of the location of four of the robberies around the time those robberies occurred. *Id.* at 6a.

The jury convicted petitioner on all the Hobbs Act counts and all but one of the firearms counts. Pet. App. 6a. The district court sentenced petitioner to 1395 months in prison. *Id.* at 7a.

3. The court of appeals affirmed. Pet. App. 1a-24a.

a. As relevant here, the court of appeals rejected petitioner's Fourth Amendment challenge to the historical cell-site records, holding that the government's acquisition of those business records was not a Fourth Amendment "search" of petitioner. Pet. App. 8a-17a.

The court of appeals emphasized that petitioner "lack[s] any property interest in cell-site records created and maintained by [his] wireless carrier." Pet. App. 12a. As the court explained, MetroPCS and Sprint "gathered [the data] in the ordinary course of business" to be used for their own purposes, such as "to find weak spots in their network and to determine whether roaming charges apply." *Id.* at 10a.

The court of appeals further concluded that petitioner had no reasonable expectation of privacy in his cellular-service providers' records of their towers' connections with his cell phone. Pet. App. 7a-13a. The court observed that "federal courts have long recognized a core distinction" between "the content of personal communications," which "is private," and "the information necessary to get those communications from point A to point B," which "is not." *Id.* at 9a. Historical cell-site records "fall on the unprotected side of this line," the court concluded, "because they contain "routing information" and "say nothing about the content of any calls." *Id.* at 10a; see *id.* at 10a-12a.

The court of appeals observed that this Court's decision in *Smith* v. *Maryland*, 442 U.S. 735 (1979), "confirm[ed] the point" that "[t]he government's collection of business records containing [historical cell-site] data * * * is not a search." Pet. App. 11a. "[I]n *Smith*," the court explained, "th[is] Court held that

the police's installation of a pen register—a device that tracked the phone numbers a person dialed from his home phone—was not a search because the caller could not reasonably expect those numbers to remain private." *Id.* at 9a-10a. Because "Smith 'voluntarily conveyed numerical information to the telephone company and exposed that information to its equipment in the ordinary course of business," the "numerical information was not protected under the Fourth Amendment." *Id.* at 12a (quoting 442 U.S. at 744) (internal quotation marks omitted). The court concluded that the same result should apply "to the locational information here" because cell-phone users voluntarily convey that data to their cellular-service providers "as a means of establishing communication" when they place or receive calls. *Ibid.* (quoting *Smith*, 442 U.S. at 741).

The court of appeals distinguished this Court's decision in *United States* v. *Jones*, 132 S. Ct. 945 (2012), which held that the government's installation of a Global-Positioning-System (GPS) tracking device on a vehicle constituted a "search" under the Fourth Amendment, *id.* at 949. See Pet. App. 13a-15a. The court of appeals emphasized that "the government action in this case"—namely, "government collection of business records"—"is very different from the government action in *Jones*." *Id.* at 13a, 14a. The court further observed that the historical cell-site data here was "as much as 12,500 times less accurate than the GPS data in *Jones*" and so could not provide the same level of detail about petitioner's location and movements. *Id.* at 14a.

The court of appeals also observed that, in enacting the SCA, Congress "struck a balance that it thinks

reasonable," Pet. App. 16a, by requiring the government to "offer[] specific and articulable facts showing that there are reasonable grounds to believe that" historical cell-site records "are relevant and material to an ongoing criminal investigation," 18 U.S.C. 2703(d). The court stated that "Congress is usually better equipped than courts are to answer the empirical questions that [new] technologies present." Pet. App. 17a. The court concluded that "[t]hese concerns favor leaving undisturbed the Congressional judgment" reflected by the SCA's "middle ground [approach] between full Fourth Amendment protection and no protection at all." *Id.* at 15a, 17a.[2]

b. Judge Stranch filed an opinion concurring in the judgment on the Fourth Amendment issue. Pet. App. 24a-32a.

Judge Stranch believed that the government's acquisition of the historical cell-site records "raise[d] Fourth Amendment concerns." Pet. App. 24a; see *id.* at 25a-29a. She "f[ound] it unnecessary to reach a definitive conclusion on the Fourth Amendment issue," however, because she concluded that the motion to suppress was properly denied under the good-faith exception to the exclusionary rule. *Id.* at 25a; see *id.* at 29a-31a. She observed that no evidence "suggest[ed] that the FBI agents who obtained the

---

[2] Because the court of appeals concluded that the government's acquisition of petitioner's historical cell-site data did not constitute a search, it did not reach the government's alternative arguments that (i) any search that occurred was constitutionally reasonable, see Gov't C.A. Br. 37-40; (ii) the good-faith exception to the exclusionary rule applies here, see *id.* at 40-42; and (iii) any error in admitting the historical cell-site data was harmless, see *id.* at 44-47.

[cell-site data] * * * pursuant to the SCA engaged in intentional misconduct." *Id.* at 31a. Because "[s]uppressing the [cell-site data] at trial would not have the requisite deterrent effect on future unlawful conduct," she concluded that the district court correctly denied the motion to suppress. *Ibid.*

ARGUMENT

Petitioner renews his claim (Pet. 10-34) that the government's acquisition of MetroPCS's and Sprint's historical cell-site records pursuant to three SCA court orders violated his Fourth Amendment rights. Petitioner further asserts (Pet. 21-26) that the lower courts are divided on the Fourth Amendment question. Those claims lack merit. The court of appeals correctly concluded that the Fourth Amendment permits the government to obtain historical cell-site data under the standard set forth in the SCA, and no conflict exists on that question. This Court has recently denied other petitions for a writ of certiorari raising Fourth Amendment challenges to the government's acquisition of historical cell-site data pursuant to SCA court orders,[3] and no reason exists for a different result here.

In any event, this case would be an unsuitable vehicle to address the Fourth Amendment question because, as the district court held and as Judge Stranch concluded in her opinion concurring in the judgment, the relevant evidence was admissible under the good-faith exception to the exclusionary rule. In addition, any error in the admission of the historical cell-site data was harmless because other evidence

---

[3] See *Davis* v. *United States*, 136 S. Ct. 479 (2015) (No. 15-146); *Guerrero* v. *United States*, 135 S. Ct. 1548 (2015) (No. 14-7103).

conclusively established petitioner's guilt. Petitioner thus could not benefit from a ruling in his favor on the Fourth Amendment question. Further review of that question is unwarranted.

1. The court of appeals correctly held that the government's acquisition of MetroPCS's and Sprint's cell-site records pursuant to court orders authorized by the SCA did not violate petitioner's Fourth Amendment rights. Petitioner has no Fourth Amendment interest in those business records. And even if he did have such an interest, the SCA procedure is constitutionally reasonable.

a. A person has no Fourth Amendment interest in records created by a communications-service provider in the ordinary course of business that pertain to the individual's transactions with the service provider.

i. The Fourth Amendment's prohibition on unreasonable searches was originally understood to be "tied to common-law trespass." *United States* v. *Jones*, 132 S. Ct. 945, 949 (2012). Since this Court's decision in *Katz* v. *United States*, 389 U.S. 347 (1967), however, the Court has held that a Fourth Amendment search may also "occur[] when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo* v. *United States*, 533 U.S. 27, 33 (2001).

The Fourth Amendment permits the government to obtain business records through a subpoena, without either a warrant or a showing of probable cause. See *Oklahoma Press Publ'g Co.* v. *Walling*, 327 U.S. 186, 194-195 (1946); see also *United States* v. *Miller*, 425 U.S. 435, 445-446 (1976). In its decisions in *Miller* and *Smith* v. *Maryland*, 442 U.S. 735 (1979), this Court further concluded that the acquisition of a busi-

ness's records does not constitute a Fourth Amendment "search" of an individual customer even when the records reflect information pertaining to that customer.

In *Miller*, the government had obtained by subpoena records of the defendant's accounts from his banks, including copies of his checks, deposit slips, financial statements, and other business records. 425 U.S. at 436-438. The banks were required to keep those records under the Bank Secrecy Act, 12 U.S.C. 1829b(d). 425 U.S. at 436, 440-441. The Court held that the government's acquisition of those records was not an "intrusion into any area in which [the defendant] had a protected Fourth Amendment interest." *Id.* at 440. The Court explained that the defendant could "assert neither ownership nor possession" of the records; rather, they were "business records of the banks." *Ibid.* The Court further rejected the defendant's argument that he had "a reasonable expectation of privacy" in the records because "they [were] merely copies of personal records that were made available to the banks for a limited purpose." *Id.* at 442. As the Court explained, it had "held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose." *Id.* at 443. Because the records obtained from the bank "contained only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," the Court concluded that the defendant had "take[n] the risk, in revealing his affairs to another,

that the information w[ould] be conveyed by that person to the Government." *Id.* at 442, 443.

In *Smith*, the Court applied the same principles to records created by a telephone company. There, the police requested that the defendant's telephone company install a pen register at its offices to record the numbers dialed from the defendant's home phone. 442 U.S. at 737. The defendant argued that the government's acquisition of the records of his dialed numbers violated his reasonable expectation of privacy and therefore qualified as a Fourth Amendment search. *Id.* at 741-742. The Court rejected that contention, concluding both that the defendant lacked a subjective expectation of privacy and that any such expectation was not objectively reasonable. *Id.* at 742-746.

The *Smith* Court first expressed "doubt that people in general entertain any actual expectation of privacy in the numbers they dial," given that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through the telephone company switching equipment that their calls are completed." 442 U.S. at 742. The Court further emphasized that "the phone company has facilities for recording this information" and "does in fact record this information for a variety of legitimate business purposes." *Id.* at 743.

The *Smith* Court went on to explain that "even if [the defendant] did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable." 442 U.S. at 743 (citation and internal quotation marks omitted). That was because "a person has no legitimate expectation of privacy in information he voluntarily turns over to

third parties." *Id.* at 743-744 (citing, *inter alia*, *Miller*, 425 U.S. at 442-444). "When [the defendant] used his phone," the Court continued, he "voluntarily conveyed numerical information to the telephone company and exposed that information to its equipment in the ordinary course of business." *Id.* at 744 (internal quotation marks omitted). The Court found no more persuasive the defendant's argument that he reasonably expected the local numbers he dialed to remain private because "telephone companies, in view of their present billing practices, usually do not record local calls" or include those numbers on their customers' monthly bills. *Id.* at 745. Because the defendant "voluntarily conveyed to [the phone company] information that it had facilities for recording and that it was free to record," the Court concluded that he had "assumed the risk that the information would be divulged to police." *Ibid.*

ii. The principles set forth in *Miller* and *Smith* resolve this case. See Pet. App. 11a-12a, 14a.

Petitioner lacks any subjective expectation of privacy in phone-company records of historical cell-site data because they are business records that MetroPCS and Sprint create for their own purposes. See Pet. App. 7a, 10a. As with the bank records in *Miller*, petitioner "can assert neither ownership nor possession" of the cell-site records. 425 U.S. at 440. Rather, the providers created the records for their own business purposes as part of the process of providing telephone service to customers. See Pet. App. 5a-7a, 10a.

As in *Smith*, moreover, cell-phone users presumably understand that their phones emit signals that are conveyed to their service providers, through facilities

close to the area of the phone's use, as a necessary incident of making or receiving calls. See, *e.g.*, *United States* v. *Davis*, 785 F.3d 498, 511 (11th Cir.) (en banc), cert. denied, 136 S. Ct. 479 (2015); *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 613 (5th Cir. 2013) (*Fifth Circuit In re Application*); Pet. App. 12a. "[A]ny cellphone user who has seen her phone's signal strength fluctuate must know that, when she places or receives a call, her phone 'exposes' its location to the nearest cell tower and thus to the company that operates the tower." Pet. App. 12a. That is why, for example, cell phones often cannot receive a signal in sparsely populated areas or underground. See *Fifth Circuit In re Application*, 724 F.3d at 613. "Although subjective expectations cannot be scientifically gauged," cell-phone users, like landline users, do not have a "general expectation" that data generated when they use telephone-company equipment "will remain secret." *Smith*, 442 U.S. at 743.

Additionally, any subjective expectation of privacy in information transmitted to a cellular-service provider by engaging its cellular network would not be objectively reasonable because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743-744. Just as a person who dials a number into a phone "voluntarily convey[s] numerical information to the telephone company and expose[s] that information to its equipment in the ordinary course of business," *id.* at 744 (internal quotation marks omitted), a cell-phone user must reveal his general location to a cell tower in order for the cellular service provider to connect a call. And a cell-

phone user thus "takes the risk, in revealing his affairs to [the cellular-service provider], that the information" he transmits in engaging the cellular network "will be conveyed by [the cellular-service provider] to the Government." *Miller*, 425 U.S. at 443. Because petitioner "voluntarily conveyed to [his cellular-service providers] information that [they] had facilities for recording and that [they] w[ere] free to record," he "assumed the risk that the information would be divulged to police." *Smith*, 442 U.S. at 745. The court of appeals therefore correctly concluded that the government's acquisition of the historical cell-site data did not constitute a Fourth Amendment search.

iii. Petitioner's arguments to the contrary (Pet. 26-32) lack merit.

Petitioner seeks to avoid (Pet. 28-29) the principles set forth in *Miller* and *Smith* by contending that cell-phone users do not voluntarily convey cell-site data to their service providers. But "[a] cell phone user voluntarily enters an arrangement with his service provider in which he knows that he must maintain proximity to the provider's cell towers in order for his phone to function." *United States* v. *Graham*, 824 F.3d 421, 430 (4th Cir.) (en banc), petitions for cert. pending, No. 16-6308 (filed Sept. 26, 2016), and No. 16-6694 (filed Oct. 27, 2016). Petitioner chose to carry a cell phone for the purpose of having his wireless provider route calls to and from him whenever he was in range of a cell tower. By "expect[ing] his phone to work," he "permitt[ed]—indeed, request[ed]—his service provider to establish a connection between his phone and a nearby cell tower," and he thus "voluntarily convey[ed] the information necessary for his ser-

vice provider to identify the [historical cell-site data] for his calls." *Ibid.*

Petitioner also errs in suggesting (Pet. 29) that *Smith* and *Miller* are inapplicable because the records at issue in this case are "exceedingly sensitive and private in ways that were not at issue in [those decisions]."[4] Petitioner provides no support for his contention that records of the cell towers to which a phone connected when placing or receiving a call are more private than, for example, the financial information contained in the "checks, deposit slips, * * * financial statements, and * * * monthly statements" the government acquired in *Miller*. 425 U.S. at 438. Although the records in *Miller* were "copies of personal records that were made available to the banks for a limited purpose," this Court nevertheless concluded that no Fourth Amendment search had occurred because the records "contain[ed] only information voluntarily conveyed to the banks and

---

[4] Petitioner's reliance for this point (Pet. 29-30) on *United States* v. *Karo*, 468 U.S. 705 (1984), and *Kyllo*, *supra*, is misplaced. In *Karo*, this Court concluded that police officers conducted a Fourth Amendment search when they used a beeper device to monitor the location of a container within a private residence. 468 U.S. at 714. Similarly, in *Kyllo*, this Court held that the use of a thermal imaging device "that is not in general public use[] to explore details of the home that would previously have been unknowable without physical intrusion" is a Fourth Amendment search. 533 U.S. at 40. In each case, the use of the device in question permitted the authorities to obtain information from inside a house that had not already been exposed to the public. See *id.* at 34-40; *Karo*, 468 U.S. at 714-716. In this case, however, petitioner had already exposed the information necessary to create the cell-site records to MetroPCS and Sprint, and the government obtained that information from MetroPCS and Sprint through lawful process.

exposed to their employees in the ordinary course of business." *Id.* at 442. That analysis applies with even greater force here because, unlike in *Miller*, the records at issue here are not even copies of documents that petitioner submitted to the cellular-service providers, and the government did not require the providers to keep those records. See *ibid.* Petitioner's argument also overlooks the "core distinction" between "the content of personal communications" and "the information necessary to get those communications from point A to point B." Pet. App. 9a. "The business records here fall on the unprotected side of this line" because they "say nothing about the content of any calls" but instead contain only "routing information." *Id.* at 10a.

Petitioner essentially objects to the fact that law-enforcement officers could *infer* from MetroPCS's and Sprint's records that petitioner was within a particular radius of a cell tower. But "an inference is not a search." *Kyllo*, 533 U.S. at 33 n.4. Law-enforcement investigators regularly deduce facts about a person's movements or conduct from information gleaned from third parties. Indeed, that is a central feature of criminal investigations. See *Donaldson* v. *United States*, 400 U.S. 517, 522 (1971) (explaining that the lack of Fourth Amendment protection for third-party business records was "settled long ago"); *id.* at 537 (Douglas, J., concurring) ("There is no right to be free from incrimination by the records or testimony of others."). For example, law-enforcement officers can infer from an eyewitness statement that a suspect was in a particular location at a particular time, from a credit-card slip that she regularly dines at a particular restaurant and was there at a particular time, and from a key-

card entry log her routine hours at a gym. But merely because facts about a person can be deduced from records or other information in the possession of third parties does not make the acquisition of that information a Fourth Amendment search of the person. Indeed, the pen-register records in *Smith* allowed a far more specific inference about the defendant's whereabouts—his presence in his home—but the Court nevertheless concluded that no Fourth Amendment search had occurred.

Petitioner suggests (Pet. 16-18, 27-28) that the Fourth Amendment principles recognized in *Smith* and *Miller* should not apply to new technologies. Although petitioner relies (Pet. 16-18) on *Jones* and *Riley* v. *California*, 134 S. Ct. 2473 (2014), those decisions did not address—much less disavow—this Court's precedents recognizing that an individual does not have a Fourth Amendment interest in a third party's records pertaining to him or in information that he voluntarily conveys to third parties. In *Jones*, the Court held that the warrantless installation and use of a GPS tracking device on a vehicle to continuously monitor its movements over the course of 28 days constituted a Fourth Amendment search. 132 S. Ct. at 948-949. In reaching that conclusion, the Court relied on the fact that the government had "physically intrud[ed] on a constitutionally protected area"—the suspect's automobile—to attach the device. *Id.* at 950 n.3. In this case, by contrast, petitioner does not contend that any such physical occupation occurred. Because the Court in *Jones* concluded that the attachment of the device constituted "a classic trespassory search," *id.* at 954, it did not reach the *Katz* inquiry or hold that tracking a person's vehicle

on public streets violates a reasonable expectation of privacy, which would represent a significant qualification of the Court's prior holding in *United States* v. *Knotts*, 460 U.S. 276, 281-282 (1983). See *Jones*, 132 S. Ct. at 953-954.

This Court's decision in *Riley* likewise does not aid petitioner's argument. *Riley* held that a law-enforcement officer generally must obtain a warrant to search the contents of a cell phone found on an arrestee. 134 S. Ct. at 2485. No question existed in *Riley* that the review of the contents of a cell phone constitutes a Fourth Amendment search; the question was whether that search fell within the traditional search-incident-to-arrest exception to the warrant requirement. See *id.* at 2482 ("The two cases before us concern the reasonableness of a warrantless search incident to a lawful arrest."); see also *id.* at 2489 n.1 (noting that "[b]ecause the United States and California agree that these cases involve *searches* incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances"). *Riley* thus presented no occasion for this Court to reconsider its longstanding view that an individual has no Fourth Amendment interest in records pertaining to an individual that are created by third parties or in information he voluntarily conveys to third parties.

Even putting aside the specific holdings of *Jones* and *Riley*, the broader privacy concerns raised in those cases (and discussed in the concurrences by Justice Alito and Justice Sotomayor in *Jones*, see 132 S. Ct. at 954-956 (Sotomayor, J., concurring); *id.* at 962-964 (Alito, J., concurring in the judgment)) do not

justify creating a novel Fourth Amendment rule here. The GPS tracking device in *Jones* allowed law-enforcement officers to use "signals from multiple satellites" to continuously track the movements of the defendant's vehicle over the course of 28 days, accurate to "within 50 to 100 feet." *Id.* at 948 (majority opinion). The information the government acquired in this case, by contrast, consisted of records indicating which of the cellular-service provider's antennas communicated with petitioner's phone only when the phone was making or receiving calls, not continuously. See Pet. App. 4a, 6a-7a. And although these records contained historical cell-site information for a 127-day period, the information revealed only that petitioner was somewhere within the specified sector of a cell tower when he made or received calls. *Id.* at 7a, 14a. According to the court of appeals' calculations, that information was "as much as 12,500 times less accurate than the GPS data in *Jones*." *Id.* at 14a-15a. This case thus presents no occasion to consider the legal implications of technology capable of "secretly monitor[ing] and catalog[ing] every single movement" an individual makes continuously "for a very long period." *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment); see *id.* at 955 (Sotomayor, J., concurring).

Likewise, this case does not touch on a central concern in *Riley*: that cell phones may contain "vast quantities of personal information" that could be used to discern "[t]he sum of an individual's private life," including information about the user's health, family, religion, finances, political and sexual preferences, and shopping habits, as well as GPS records of the user's "specific movements down to the minute, not

only around town but also within a particular building." 134 S. Ct. at 2485, 2489, 2490. As explained, the historical cell-site records obtained in this case revealed only that petitioner (or someone using his phone) was in "a 3.5 million square-foot to 100 million square-foot area" when placing or receiving a call. Pet. App. 14a. The records did not (and could not) reveal any information stored on petitioner's phone or permit law-enforcement officers to learn the sort of detailed personal facts that the Court identified in *Riley*.

Petitioner essentially seeks a rule that he has a personal Fourth Amendment interest in the record of his transaction with a business from which his location can be approximately inferred. No recognized Fourth Amendment doctrine supports that contention.[5] The court of appeals therefore correctly held that under this Court's precedents, petitioner has no valid Fourth Amendment interest in records of his calls created by MetroPCS and Sprint for their own business purposes.

b. Even if petitioner could establish that he has a novel Fourth Amendment interest in the records created and held by MetroPCS and Sprint, the govern-

---

[5] Petitioner cites (Pet. 26-27) a variety of cases that did not involve the third-party doctrine to support his contention that privacy interests may survive even when "another person has access to or control over private records." None of those cases involved business records created by a third party based on information voluntarily conveyed to the business. For example, *Ferguson* v. *City of Charleston*, 532 U.S. 67 (2001), involved urine tests conducted by state hospital staff that "were indisputably searches within the meaning of the Fourth Amendment." *Id.* at 76. The other cited cases are equally inapposite.

ment's acquisition of those records was reasonable and therefore complied with the Fourth Amendment.

"As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'" *Maryland* v. *King*, 133 S. Ct. 1958, 1969 (2013) (citation omitted). A "warrant is not required to establish the reasonableness of *all* government searches; and when a warrant is not required (and the Warrant Clause therefore not applicable), probable cause is not invariably required either." *Vernonia Sch. Dist. 47J* v. *Acton*, 515 U.S. 646, 653 (1995). In deciding whether a warrantless search is permissible, this Court "balance[s] the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable." *King*, 133 S. Ct. at 1970 (citation omitted). In addition, in a case that challenges a federal statute under the Fourth Amendment, this Court applies a "strong presumption of constitutionality" to the statute, "especially when it turns on what is 'reasonable'" within the meaning of the Fourth Amendment. *United States* v. *Watson*, 423 U.S. 411, 416 (1976) (citation omitted). In light of those principles, even if the acquisition of MetroPCS's and Sprint's records pertaining to petitioner's calls qualified as a Fourth Amendment search, that acquisition would be constitutionally reasonable. That follows for two independently sufficient reasons.

First, as discussed above, this Court has held that subpoenas for records do not require a warrant based on probable cause, even when challenged by the party to whom the records belong. See *Miller*, 425 U.S. at 446 (reaffirming the "traditional distinction between a search warrant and a subpoena"); see also *Oklahoma*

Press Publ'g Co., 327 U.S. at 209. It follows that the SCA procedure for obtaining the business records at issue here is constitutionally reasonable, because the SCA provides more substantial privacy protections than an ordinary judicial subpoena. See *Davis*, 785 F.3d at 505-506 (describing SCA privacy-protection provisions). In particular, the SCA "raises the bar" for obtaining historical cell-site records, *id.* at 505, by requiring the government to establish "*specific and articulable facts* showing that there are reasonable grounds to believe that * * * the records or other information sought[ ] are relevant and material to an ongoing criminal investigation," 18 U.S.C. 2703(d) (emphasis added). In contrast, an ordinary subpoena requires only a "court's determination that the investigation is authorized by Congress, [that it] is for a purpose Congress can order, [that] the documents sought are relevant to the inquiry," and that the "specification of the documents to be produced [is] adequate, but not excessive, for the purposes of the relevant inquiry." *Oklahoma Press Publ'g Co.*, 327 U.S. at 209. Given that "[a] legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way," *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment), Congress's considered effort in the SCA to augment the privacy protections that this Court has found sufficient for judicial subpoenas complies with the Fourth Amendment. See Pet. App. 15a-17a.

Second, traditional standards of Fourth Amendment reasonableness independently confirm that a Section 2703(d) court order is a reasonable mechanism for obtaining a cellular-service provider's historical

cell-site records. As discussed above, under traditional Fourth Amendment standards, petitioner had no legitimate expectation of privacy in the third-party business records at issue here. But even if this Court were to depart from that settled framework and hold that an individual can assert a Fourth Amendment interest in records created by a third party that pertain to a transaction he engaged in with the third party, petitioner could at most assert only a diminished expectation of privacy in those records. That is a factor that this Court has said "may render a warrantless search or seizure reasonable." *King*, 133 S. Ct. at 1969 (citation omitted). And any invasion of petitioner's assumed privacy interest was minimal, given the imprecise nature of the location information that could be inferred from the historical cell-site records at issue here, which could not have enabled law-enforcement officers to pinpoint petitioner's location and could not have revealed other personal facts about him. See Pet. App. 14a-15a (discussing these factors); *Davis*, 785 F.3d at 516 (same).

On the other side of the reasonableness balance, the government has a compelling interest in obtaining historical cell-site records using a Section 2703(d) court order, rather than a warrant, because, like other investigative techniques that involve seeking information from third parties about a crime, this evidence is "particularly valuable during the early stages of an investigation, when the police [may] lack probable cause and are confronted with multiple suspects." *Davis*, 785 F.3d at 518. Society has a strong interest in both promptly apprehending criminals and exonerating innocent suspects as early as possible during an investigation. See *United States* v. *Salerno*, 481 U.S.

739, 750-751 (1987); *King*, 133 S. Ct. at 1974. In addition, the SCA ensures judicial scrutiny of the government's basis for obtaining an order, so the government may obtain such orders only in circumstances where the asserted governmental interest in acquiring the records has been examined by a neutral magistrate.

In short, "a traditional balancing of interests amply supports the reasonableness of the [SCA] order[s] at issue here." *Davis*, 785 F.3d at 518.

2. Petitioner contends (Pet. 21-26) that lower courts are divided over whether the Fourth Amendment requires the government to obtain a warrant before acquiring a cellular-service provider's historical cell-site records pertaining to a particular user. That is incorrect. The decision below does not conflict with any other decision of another circuit or state high court.

a. All courts of appeals to have considered the question presented have concluded, in accordance with the Sixth Circuit below, that no Fourth Amendment violation occurs when the government acquires historical cell-site data pursuant to an SCA order. See *Graham*, 824 F.3d at 425-438 (4th Cir.); *Davis*, 785 F.3d at 506-516 (11th Cir.); *Fifth Circuit In re Application*, 724 F.3d at 609-615 (5th Cir.); Pet. App. 17a.[6]

b. Petitioner asserts (Pet. 14, 22-23) that the decision below conflicts with the Third Circuit's decision in *In re Application of the U.S. for an Order Direct-*

---

[6] Petitions for a writ of certiorari from the Fourth Circuit's decision in *Graham* are currently pending. See Nos. 16-6308 (filed Sept. 26, 2016) and 16-6694 (filed Oct. 27, 2016). Those petitions raise a similar Fourth Amendment challenge to the government's acquisition of historical cell-site data.

ing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (2010) (*Third Circuit In re Application*). But the Third Circuit addressed only the *statutory* standard for obtaining cell-site records under the SCA. *Id.* at 308-319. The Third Circuit "h[eld] that [historical cell-site data] from cell phone calls is obtainable under a [Section] 2703(d) order and that such an order does not require the traditional probable cause determination." *Id.* at 313. The court further interpreted the SCA to grant judges discretion "to require a warrant showing probable cause" pursuant to Section 2703(c)(1)(A), although the court stated that such an option should "be used sparingly because Congress also included the option of a [Section] 2703(d) order." *Id.* at 319. But the court did not consider—let alone adopt—petitioner's proposed rule that the Fourth Amendment *requires* the government to obtain a warrant to acquire historical cell-site data.

Petitioner emphasizes (Pet. 22-23) the Third Circuit's statement that "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way." *Third Circuit In re Application*, 620 F.3d at 317. But the Third Circuit made that observation simply to support its interpretation of the SCA. And while the court noted "the possibility" that the disclosure of historical cell-site data could "implicate the Fourth Amendment * * * if it would disclose location information about the interior of a home," *ibid.*, that suggestion would not aid petitioner here, because the evidence he sought to suppress did not (and could not) disclose anything about the interior of his home. In any event, the Third Circuit's suggestion does not amount to a

constitutional holding that would place it in conflict with the Fourth, Fifth, Sixth, and Eleventh Circuits.[7]

c. Petitioner also contends (Pet. 24-26) that the court of appeals' decision conflicts with the D.C. Circuit's decision in *United States* v. *Maynard*, 615 F.3d 544 (2010), aff'd in part on other grounds *sub nom. United States* v. *Jones*, 132 S. Ct. 945 (2012). But *Maynard* involved the government's installation and use of a GPS tracking device on the defendant's car, not the acquisition of records that a third party had created and stored for its own business purposes. See *id.* at 555. Indeed, *Maynard* specifically recognized the continuing validity of the principles applied in *Smith*. See *id.* at 561; see also *Reporters Comm. for Freedom of the Press* v. *American Tel. & Tel. Co.*, 593 F.2d 1030, 1043 (D.C. Cir. 1978), cert. denied, 440 U.S. 949 (1979).

d. Petitioner further errs in contending that "state high courts are divided" on the question presented in this case. Pet. 21 (capitalization omitted).[8] Petitioner

---

[7] The Third Circuit recently heard oral argument in a case that involves a Fourth Amendment challenge to the government's acquisition of historical cell-site data pursuant to an SCA order under Section 2703(d). See *United States* v. *Stimler*, Nos. 15-4053, 15-4094, and 15-4095 (argued Jan. 25, 2017). That case may provide the Third Circuit with an opportunity to revisit its empirical assumption from six years ago that "it is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information." *Third Circuit In re Application*, 620 F.3d at 317 (emphasis omitted).

[8] Petitioner also cites (Pet. 14, 23) a decision from the Indiana Court of Appeals, but that decision was recently vacated when the Supreme Court of Indiana granted discretionary review. See *Zanders* v. *State*, 58 N.E.3d 254, vacated and transfer granted, 62 N.E.3d 1202 (Ind. 2016). In any event, a conflict with a decision of

cites (Pet. 23-24) two decisions in which state courts of last resort required warrants to obtain cell-site records, but both of those decisions relied expressly on state law. See *Commonwealth* v. *Augustine*, 4 N.E.3d 846, 858, 865-866 (Mass. 2014) (Massachusetts Declaration of Rights); *State* v. *Earls*, 70 A.3d 630, 644 (N.J. 2013) (New Jersey Constitution). In addition, petitioner cites (Pet. 23-24) the Florida Supreme Court's decision in *Tracey* v. *State*, 152 So. 3d 504 (2014), but that case involved the use of prospective, "*real time* cell site location information," and the court made clear that its decision did not encompass historical cell-site records like those at issue here. *Id.* at 515, 525-526 (emphasis added). Petitioner also points to (Pet. 23-24) several state statutes, but those statutes do not reflect any judicial conflict over the meaning of the Fourth Amendment. To the contrary, they fortify the view that legislatures are best positioned to balance privacy interests and law-enforcement needs in light of new technologies, as Congress did in the SCA. See *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment); see Pet. App. 15a-17a.

3. In any event, this case is not a suitable vehicle to consider whether the government's acquisition of historical cell-site data violated the Fourth Amendment because the district court correctly denied the motion to suppress based on the good-faith exception to the exclusionary rule and because any error in admitting the cell-site data was harmless.

a. As this Court has explained, the exclusionary rule is a "judicially created remedy" that is "designed to deter police misconduct rather than to punish the

---

an intermediate state appellate court does not warrant this Court's review.

errors of judges and magistrates." *United States* v. *Leon*, 468 U.S. 897, 906, 916 (1984). "As with any remedial device, application of the exclusionary rule properly has been restricted to those situations in which its remedial purpose is effectively advanced." *Illinois* v. *Krull*, 480 U.S. 340, 347 (1987). The rule therefore does not apply "where [an] officer's conduct is objectively reasonable" because suppression "cannot be expected, and should not be applied, to deter objectively reasonable law enforcement activity." *Leon*, 468 U.S. at 919. For that reason, "evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." *Ibid.* (citation omitted).

As the district court correctly held, Pet. App. 38a n.1, and as Judge Stranch recognized in her opinion concurring in the judgment, *id.* at 29a-31a, even if the government's collection of the historical cell-site data constituted a search in violation of the Fourth Amendment, the evidence was properly admitted at trial pursuant to the good-faith exception to the exclusionary rule. As Judge Stranch emphasized, "there is nothing to suggest that the FBI agents who obtained [the historical cell-site data] * * * pursuant to the SCA engaged in any intentional misconduct." *Id.* at 31a. This Court has held that the good-faith exception applies to "officer[s] acting in objectively reasonable reliance on a statute," later deemed unconstitutional, that authorizes warrantless administrative searches. *Krull*, 480 U.S. at 349; see *id.* at 342. It follows *a fortiori* that officers act reasonably in relying on a

statute that authorizes the acquisition of records only pursuant to an order issued by a neutral magistrate.

At the time the records were acquired in petitioner's case, moreover, no binding appellate decision (or holding of any circuit) had suggested, much less held, that the SCA was unconstitutional as applied to historical cell-site records. Given that, officers were entitled to rely on the presumption that acts of Congress are constitutional. Cf. *Davis* v. *United States*, 131 S. Ct. 2419, 2429 (2011) ("Evidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule."). Judge Stranch accordingly correctly concluded that "[s]uppressing the [historical cell-site data] at trial would not have the requisite deterrent effect on future unlawful conduct and application of the exclusionary rule is therefore inappropriate." Pet. App. 31a.

b. In addition, even if the historical cell-site data should have been suppressed, any error in admitting that evidence at trial was harmless. See *Neder* v. *United States*, 527 U.S. 1, 18 (1999) (observing that constitutional error is harmless when it is "clear beyond a reasonable doubt that a rational jury would have found the defendant guilty absent the error"). The information provided by the historical cell-site data was merely cumulative of other uncontroverted evidence at trial that placed petitioner near the robbery scenes. See Gov't C.A. Br. 44-47 (describing evidence). That evidence included surveillance tape video showing petitioner near the site of one robbery, see *id.* at 45-46, as well as testimony from eyewitness accomplices who described petitioner's involvement in and presence at the scene of the other robberies, see

id. at 46-47; see also Pet. App. 5a (describing testimony from accomplices "that [petitioner] organized most of the robberies and often supplied the guns"). In light of the other evidence establishing petitioner's involvement in the robberies and his location at the relevant times, it is clear that the jury would have returned a guilty verdict even if the historical cell-site data had not been admitted at trial. Indeed, the jury convicted petitioner on two robbery counts for which the government had *not* introduced any historical cell-site data.

Because petitioner would not obtain relief even if this Court were to rule in his favor on the Fourth Amendment question, review of that question is not warranted in this case.

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted.

NOEL J. FRANCISCO
Acting Solicitor General
KENNETH A. BLANCO
Acting Assistant Attorney General
JENNY C. ELLICKSON
Attorney

JANUARY 2017

RECORD AND BRIEFS

No. 16-402

FILED
FEB 10 2017
OFFICE OF THE CLERK
SUPREME COURT, U.S.

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

—v.—

UNITED STATES OF AMERICA,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

REPLY TO BRIEF IN OPPOSITION

Harold Gurewitz
GUREWITZ & RABEN, PLC
333 W. Fort Street, Suite 1400
Detroit, MI 48226

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
AMERICAN CIVIL LIBERTIES
UNION FUND OF MICHIGAN
2966 Woodward Ave.
Detroit, MI 48201

Nathan Freed Wessler
Counsel of Record
Ben Wizner
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

David D. Cole
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
915 15th Street, NW
Washington, D.C. 20005

Library of Congress
Law Library

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii
REPLY TO BRIEF IN OPPOSITION 1

TABLE OF AUTHORITIES

CASES

Arizona v. Hicks, 480 U.S. 321 (1987) 9

Davis v. United States, 564 U.S. 229 (2011) 11

Ferguson v. City of Charleston, 532 U.S. 67 (2001) ... 9

Illinois v. Krull, 480 U.S. 340 (1987) 10

In re Application for Telephone Info. Needed for Criminal Investigation, 119 F. Supp. 3d 1011 (N.D. Cal. 2015) 3

In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) 4

In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304 (3d Cir. 2010) 2, 4

Jones v. United States, 357 U.S. 493 (1958) 10

Kyllo v. United States, 533 U.S. 27 (2001) 7

Riley v. California, 134 S. Ct. 2473 (2014) 1, 5, 9

Smith v. Maryland, 442 U.S. 735 (1979) 3, 5

Tracey v. State, 152 So. 3d 504 (Fla. 2014) 3

United States v. Davis, 754 F.3d 1205 (11th Cir. 2014) 4

United States v. Graham, 824 F.3d 421 (4th Cir. 2016) 3, 4

United States v. Graham, 796 F.3d 332 (4th Cir. 2015) 3, 4, 6

United States v. Jones, 565 U.S. 400 (2012) 5

United States v. Karo, 468 U.S. 705 (1984) 8

United States v. Leon, 468 U.S. 897 (1984)..... 11

United States v. Miller, 425 U.S. 435 (1976) 3

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010). 12

CONSTITUTION & STATUTES

U.S. Const. amend. IV .....*passim*

Stored Communications Act.....*passim*

18 U.S.C. § 2703 *et seq.* 2

18 U.S.C. § 2703(c)(1)(a) 11

18 U.S.C. § 2703(d)..... 2, 11

Cal. Penal Code § 1546.1(b)..... 8

12 R.I. Gen. Laws § 12-32-2..... 8

RULES

S.Ct. Rule 10(c) 3

OTHER AUTHORITIES

AT&T, *Transparency Report* (2016) 11

Sprint, *Sprint Corporation Transparency Report* (July 2016) 12

T-Mobile, *Transparency Report for 2015* (2016);..... 12

Verizon, *Verizon's Transparency Report 2H 2016*... 12

REPLY TO BRIEF IN OPPOSITION

When the Stored Communications Act ("SCA") was enacted in 1986, cell phones cost over $3,000, were the size of a large brick, could connect to only fragmentary cellular networks, and were used by very few people. Pet. 33. [1] Now, 95 percent of Americans own a cell phone, [2] and cellular tower coverage spans from coast to coast.

The government's position is that two cases from the 1970s, decided before the SCA was passed and before cell phones were available, permit law enforcement to obtain unlimited cell site location information ("CSLI") without a warrant. The government minimizes the split with the Third Circuit and downplays the importance of the issues at stake. Yet, this Court and lower courts have recognized that Fourth Amendment cases from a prior era cannot be applied mechanically to "modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014) (refusing to extend to cell phones the search-incident-to-arrest exception to the warrant requirement).

The government urges that the Sixth Circuit's approach to the Fourth Amendment—allowing

---

[1] *See also* Verizon, *Celebrating 30th Anniversary of First Commercial Cell Phone Call* (Oct. 11, 2013), https://www.verizon.com/about/news/celebrating-30th-anniversary-first-commercial-cell-phone-call.

[2] Pew Research Center, *Mobile Fact Sheet* (2017), http://www.pewinternet.org/fact-sheet/mobile/.

expansive warrantless searches and seizures based on a standard well short of probable cause—be permitted to stand. The issues involved in this case are of national importance. They affect all of us, and they have been thoroughly aired in the lower courts. This Court's review is warranted.

1. As explained in the Petition, the Sixth Circuit is in conflict with the Third Circuit on the central Fourth Amendment questions in this case. Pet. 22–23. The Third Circuit's opinion in *In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304 (3d Cir. 2010) ["*Third Circuit CSLI Opinion*"], assessed, *inter alia*, whether magistrate judges have the discretion to reject applications for historical CSLI submitted pursuant to 18 U.S.C. § 2703(d), and instead to insist on warrant applications.

Answering that question was not merely an exercise in statutory interpretation, as the government claims, BIO 27, but also involved interpretation and application of the Fourth Amendment. 620 F.3d at 312–13, 317–19. The Third Circuit first engaged in statutory analysis, holding that under the plain language of § 2703, magistrate judges have discretion to reject applications for § 2703(d) disclosure orders if they determine that Fourth Amendment privacy interests necessitate the protections of a warrant. *Id.* at 315–17, 319. The court then went on to address the government's contention "that no CSLI can implicate constitutional protections because the subscriber has shared its information with a third party, i.e., the

communications provider. For support, the Government cites *United States v. Miller*, 425 U.S. 435[] (1976), . . . [and] *Smith v. Maryland*, 442 U.S. 735[] (1979)." *Id.* at 317. In direct contrast to the Sixth Circuit in the decision below, the Third Circuit rejected the government's argument, noting that the third-party doctrine does not apply because "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way." *Id.* Other courts have subsequently cited the Third Circuit for this conclusion. *See Tracey v. State*, 152 So. 3d 504, 522 (Fla. 2014); *In re Application for Telephone Info. Needed for Criminal Investigation*, 119 F. Supp. 3d 1011, 1029 (N.D. Cal. 2015).

This case also presents "an important question of federal law that has not been, but should be, settled by this Court." Rule 10(c). As explained in the Petition, the large volume of law enforcement requests for CSLI and the conflicting patchwork of legal standards governing access to it require resolution by this Court. Pet. 12–24. Courts of appeals have exhaustively debated the issues at stake. In four separate opinions, eight courts of appeals judges have explained their conclusion that there is a reasonable expectation of privacy in historical CSLI, and that the third-party doctrine does not apply. *United States v. Graham*, 824 F.3d 421, 441 (4th Cir. 2016) (en banc) (Wynn, J., dissenting in part and concurring in the judgment, joined by Floyd & Thacker, JJ.); *United States v. Graham*, 796 F.3d 332, 338 (4th Cir. 2015) (Davis, J., joined by Thacker, J.), *rev'd en banc*, 824 F.3d 421; *United States v. Davis*, 785 F.3d 498, 500 (11th Cir. 2015) (en banc) (Martin, J., dissenting, joined by Jill

Pryor, J.); *United States v. Davis*, 754 F.3d 1205, 1208 (11th Cir. 2014) (Sentelle, J., joined by Martin & Dubina, JJ.), *rev'd en banc*, 785 F.3d 498. Another five judges have explained that requests for historical CSLI raise substantial Fourth Amendment issues, without deciding whether the warrant requirement applies. Pet. App. 24a (Stranch, J., concurring); *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 615 (5th Cir. 2013) (Dennis, J., dissenting) ["*Fifth Circuit CSLI Opinion*"]; *Third Circuit CSLI Opinion*, 620 F.3d at 305 (Sloviter, J., joined by Roth, J.); *id.* at 319 (Tashima, J., concurring). In six opinions, 23 courts of appeals judges have concluded that there is no reasonable expectation of privacy in historical CSLI, with many of those explaining that they felt they lacked authority to part company with this Court's third-party doctrine precedents. Pet. App. 1a (Kethledge, J., joined by Guy, J.); *Graham*, 824 F.3d at 424 (Motz, J., joined by Traxler, C.J., Wilkinson, Niemeyer, King, Gregory, Shedd, Duncan, Agee, Keenan, Diaz & Harris, JJ.); *Graham*, 796 F.3d at 378 (Motz, J., dissenting in part); *Davis*, 785 F.3d at 500 (Hull, J., joined by Ed Carnes, C.J., Tjoflat, Marcus, & Julie Carnes, JJ.); *id.* at 519 (William Pryor, J., concurring); *Fifth Circuit CSLI Opinion*, 724 F.3d at 602 (Clement, J., joined by Reavley, J.). Other judges have concurred in this outcome but have written separately to raise concerns about the implications of applying this Court's third-party–doctrine cases to such sensitive data. *See Davis*, 785 F.3d at 521 (Jordan, J., concurring, joined by Wilson, J.); *id.* at 524 (Rosenbaum, J., concurring). This thorough vetting of the question presented coupled with the conflict between the Third and Sixth

Circuits provides this Court with a more than sufficient basis for review.

2. The government contends that *United States v. Miller* and *Smith v. Maryland* are controlling. For the reasons set forth in the Petition, these analog-era decisions do not dictate the outcome of this digital-era case. Pet. 28–32. As the various opinions in *United States v. Jones*, 565 U.S. 400 (2012), and *Riley v. California*, 134 S. Ct. 2473 (2014), demonstrate, "any extension of th[e] reasoning [from older Fourth Amendment cases] to digital data has to rest on its own bottom." *Riley*, 134 S. Ct. at 2489; *see also Jones*, 565 U.S. at 420, 430 (Alito, J., concurring in the judgment) ("[I]t is almost impossible to think of late–18th-century situations that are analogous to what took place in this case . . . [S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."). Among the principles that require reexamination are the third-party doctrine and the question of what constitutes a reasonable expectation of privacy in an increasingly digital world. *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

The government's "mechanical application," *Riley*, 134 S. Ct. at 2484, of *Miller* and *Smith* "appears to admit to no limitation on the quantity of records or the length of time for which such records may be compelled." Pet. App 29a. The government's

position therefore would subject to warrantless search "a staggering amount of information that surely must be protected under the Fourth Amendment," from personal emails and cloud-stored documents, to detailed and intimate internet browsing and search histories. *Davis*, 785 F.3d at 535 (Martin, J., dissenting). This Court should clarify the reach of precedents now four decades old to the voluminous and exceedingly sensitive digital records that twenty-first-century Americans cannot avoid creating as they go about their daily lives.

3. The government understates the privacy implications of the disclosure order in this case when it says that sensitive location information can only be "approximately inferred" from the CSLI records. BIO 22. The government itself characterized those records very differently at trial, arguing to the jury that the records placed Petitioner's phone "right where the first robbery was at the exact time of the robbery, the exact sector" and that he was "right in the right sector before the Radio Shack in Highland Park." Pet. 8 (citing trial transcript). Given that the government's trial strategy expressly relied on the accuracy of at least 16 of Petitioner's location data points that it believed corroborated its theory of the case, *see* Pet. App. 74a–89a, it cannot now credibly suggest that the remaining thousands of location points covering months of phone calls reveal nothing private about Petitioner's life. Those records reveal "much information about [a person's] day-to-day life that most of us would consider quintessentially private," including patterns of movement, whether she slept at home or elsewhere, and more. *Davis*, 785 F.3d at 540 (Martin, J., dissenting); *see also Graham*, 796 F.3d at 348 ("Much like long-term GPS

monitoring, long-term location information disclosed in cell phone records can reveal both a comprehensive view and specific details of the individual's daily life."); Electronic Frontier Foundation, et al., Amici Br. ["EFF Br."] 15–17. Longer-term data about Petitioner's locations and movements reveals information that society recognizes as justifiably private, and warrantless acquisition of this information violates the Fourth Amendment.

It is not dispositive that some cell site data is less precise than the GPS data at issue in *Jones*. *See* BIO 21. The size of cell site sectors varies widely. Some CSLI data points will locate a person relatively precisely, and others more approximately. EFF Br. 10–11. There is no way for an officer to know in advance whether a suspect's CSLI will reveal more or less precise location information, thus necessitating the protection of a warrant. *Cf. Kyllo v. United States*, 533 U.S. 27, 39 (2001). Moreover, as Judge Stranch explained, "precision is not the only variable with legal significance": duration and comprehensiveness of the surveillance also matter. Pet. App. 27a. The *four months* of location data collected here "far exceeds the threshold" of longer-term tracking identified in previous cases. Pet. App. 29a. And as *amici* explain, the precision and volume of CSLI data is constantly increasing, rendering all the more pressing the need for this Court to weigh in. EFF Br. 10–11.

Nor is the privacy violation mitigated because conclusions about an individual's exact location or activity based on CSLI records will sometimes rest on inferences. *See* BIO 18–19. As this Court has

explained, "the novel proposition that inference insulates a search is blatantly contrary to *United States v. Karo*, 468 U.S. 705[] (1984), where the police 'inferred' from the activation of a beeper that a certain can of ether was in the home." *Kyllo*, 533 U.S. at 36. The introduction of an inferential step to reveal otherwise-protected information does not reduce the intrusion on privacy nor absolve the government from complying with the warrant requirement.

Indeed, in recognition of the serious privacy concerns at stake, a number of states require a warrant for law enforcement access to historical CSLI. Pet. 23 (citing state statutes); *see also* Cal. Penal Code § 1546.1(b); 12 R.I. Gen. Laws § 12-32-2. These states' recognition of the expectation of privacy in CSLI supports application of the warrant requirement here. Far from suggesting that the Court should defer to legislative judgements on the constitutional question before it, *see* BIO 24; Pet. App. 16a–17a, these legislative enactments evidence the growing societal understanding that cell phone location records should be shielded from warrantless search. That understanding further supports the conclusion that there is a reasonable expectation of privacy in CSLI.

4. The government argues that even if there is a privacy interest in CSLI, the warrantless search and seizure of the data is reasonable under the Fourth Amendment. BIO 22–26. But its analogy to subpoenas of business records and papers proves too much. The government's position would allow it to warrantlessly acquire a breathtaking amount of data about a person merely by subpoenaing a third

party connected to one's cell phone. That data includes not just the location information at issue in this case, but the books one orders on Amazon, the medical data one shares with a third-party health application, the political websites one visits, the smartphone applications one downloads, the newspapers and articles one chooses to read, the pictures one stores in the cloud, the music one purchases, even the heart-rate data gathered by a smartwatch and uploaded to the cloud. Under the government's view, an individual's use of a cell phone will enable the government to not only "reconstruct someone's specific movements down to the minute" without a warrant, *Riley*, 134 S. Ct. at 2490, but to reconstruct what that person was reading, playing, listening to, or doing at that specific place.

For the same reason, the government's argument that individuals have a "diminished expectation of privacy in those records" must fail. BIO 25. Otherwise, we will be forced to choose between using our cell phones as normal members of society and retaining our privacy. The government's interest in stopping crime, BIO 25–26, is present in all cases; far from diminishing the privacy expectation, it is precisely that interest that creates the risk of police overreaching and requires application of the warrant requirement as a bulwark of privacy. *Ferguson v. City of Charleston*, 532 U.S. 67, 81 (2001) (warrantless search is unreasonable where the purpose of the search "is ultimately indistinguishable from the general interest in crime control."); *see also Arizona v. Hicks*, 480 U.S. 321, 328 (1987) (explaining that the Court would not "send police and judges into a new thicket of Fourth Amendment law" where a search did not require

probable cause). The government does not contend, nor could it, that this case falls under any specific exception to the warrant requirement such as exigency or "special needs."

The claim that such a far-reaching intrusion on a reasonable expectation of privacy is reasonable without a warrant is a novel and dangerous approach to the Fourth Amendment, and should be rejected by this Court. *Jones v. United States*, 357 U.S. 493, 499 (1958) (exceptions to the warrant requirement are to be "jealously and carefully drawn").

5. Because the court of appeals did not rule on whether the good-faith exception to the exclusionary rule applies,[3] this case is a clean vehicle for this Court to consider the question presented. The absence of a good-faith ruling distinguishes this case from *Davis*, in which the Court denied certiorari last term. *See Davis*, 785 F.3d at 518 n.20, *cert. denied*, 136 S. Ct. 479 (2015). In this case, application of the good-faith exception should be decided in the first instance by the court of appeals on remand.[4]

In any event, there are strong reasons not to expand the good-faith exception to prosecutors. Unlike the statute at issue in *Illinois v. Krull*, 480 U.S. 340 (1987), the statute here gave prosecutors the option of obtaining a warrant supported by

---

[3] The district court also did not provide a reasoned ruling addressing the good-faith exception, invoking the doctrine only in a single cursory footnote. Pet. App. 38a n.1.

[4] The court of appeals likewise did not reach decision on the government's argument that admission of the CSLI evidence was harmless error. That issue, too, should be addressed on remand.

probable cause. 18 U.S.C. § 2703(c)(1)(a). And, unlike police on the street, prosecutors, as officers of the court, are expected to scrupulously assess the Fourth Amendment interests at stake. *Cf. United States v. Leon*, 468 U.S. 897, 921 (1984). Prosecutors who choose not to seek a warrant where such a route is fully available assume the risk of suppression that flows from that decision. No decision of this Court has ever expanded the exception to a prosecutor under such circumstances.

Even if applicable, however, invocation of the good-faith exception is not a reason to deny the petition. Otherwise, the government's decision to obtain historical CSLI without seeking a warrant will be effectively insulated from appellate review. *Compare Davis v. United States*, 564 U.S. 229, 247 (2011) ("[T]he good-faith exception in this context will not prevent judicial reconsideration of prior Fourth Amendment precedents."). Given the policies of cellular service providers, the government will *always* invoke the good-faith exception because it will never be able to obtain CSLI without adhering to the court-order provision of 18 U.S.C. § 2703(d) or demonstrating an emergency that precludes such process, *see id.* § 2702(c)(4). *See, e.g.*, AT&T, *Transparency Report* 7 (2016) [5] ("[For historical location information] we require a General Court Order, search warrant, or probable cause court order, depending on the applicable state and federal laws."); *accord* Sprint, *Sprint Corporation Transparency*

[5] http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_TransparencyReport_July2016.pdf.

Report 2 (July 2016)[6]; T-Mobile, *Transparency Report for 2015*, at 2 (2016) [7] ; Verizon, *Verizon's Transparency Report 2H 2016*[8]. If application of the good-faith exception were to insulate Fourth Amendment violations from review, "the government would be given *carte blanche* to violate constitutionally protected privacy rights, provided, of course, that a statute [or court order] supposedly permits them to do so. The doctrine of good-faith reliance should not be a perpetual shield against the consequences of constitutional violations." *United States v. Warshak*, 631 F.3d 266, 282 n.13 (6th Cir. 2010).

Respectfully Submitted,

Nathan Freed Wessler
Counsel of Record
Ben Wizner
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

---

[6] http://goodworks.sprint.com/content/1022/files/Transaparency%20Report%20July2016.pdf.

[7] https://newsroom.t-mobile.com/content/1020/files/2015Transparency Report.pdf.

[8] https://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2017/01/Transparency-Report-US-2H-2016.pdf.

David D. Cole
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
915 15th Street, NW
Washington, D.C. 20005

Harold Gurewitz
GUREWITZ & RABEN, PLC
333 W. Fort Street,
Suite 1400
Detroit, MI 48226

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
AMERICAN CIVIL LIBERTIES
UNION FUND OF
MICHIGAN
2966 Woodward Ave.
Detroit, MI 48201

Dated: February 10, 2017

RECORD AND BRIEFS

Supreme Court, U.S.
FILED
OCT 28 2016
OFFICE OF THE CLERK

No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

PETITIONER,

v.

UNITED STATES OF AMERICA,

RESPONDENT.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Sixth Circuit

BRIEF FOR THE CATO INSTITUTE AS *AMICUS CURIAE* IN SUPPORT OF PETITIONER

Jim Harper
Counsel of Record
Ilya Shapiro
CATO INSTITUTE
1000 Mass. Ave. N.W.
Washington, D.C. 20001
(202) 842-0200
jharper@cato.org

October 28, 2016

Library of Congress
Law Library

QUESTION PRESENTED

Whether the warrantless seizure and search of a cell phone user's historical records, revealing his or her location and movements over the course of 127 days, is permitted by the Fourth Amendment.

TABLE OF CONTENTS

QUESTION PRESENTED i

TABLE OF AUTHORITIES iv

INTEREST OF *AMICUS CURIAE* 1

INTRODUCTION AND SUMMARY OF ARGUMENT 1

ARGUMENT 4

I. THIS COURT SHOULD APPLY THE TERMS OF THE FOURTH AMENDMENT IN ALL FOURTH AMENDMENT CASES 4

II. THIS COURT SHOULD RETURN TO APPLYING THE TERMS OF THE FOURTH AMENDMENT IN COMMUNICATIONS AND DATA CASES, ESCHEWING THE UNSOUND "REASONABLE EXPECTATION OF PRIVACY" TEST 8

A. *Ex Parte Jackson* Protected Communications in Transit by Protecting Papers and Effects as Such 9

B. *Olmstead* Involved Seizures and Searches of a Wire and Electronic Papers/Effects 10

C. The *Katz* Majority Inarticulately Applied the Fourth Amendment's Terms to a Shrouded Oral Communication 12

D. The Ills of the "Reasonable Expectation of Privacy" Test 13

E. Corollaries of the "Reasonable Expectation of Privacy" Test are Even Worse 14

III. THIS COURT'S RECENT CASES ARE A FRAMEWORK FOR ADMINISTERING THE FOURTH AMENDMENT IN A RELIABLE AND JURIDICAL WAY 18

A. *Jones* was a Seizure Case 19

B. *Kyllo* is a Modern Search Case 20

C. "Their Persons, Houses, Papers, and Effects" 21

CONCLUSION 24

TABLE OF AUTHORITIES

Page(s)

Cases

ACLU v. Clapper,
785 F.3d 787 (2d Cir. 2015) 19

Brendlin v. California,
551 U.S. 249 (2007) 6

California Bankers Association v. Shultz,
416 U.S. 21 (1974) 16

Chimel v. California,
395 U.S. 752 (1969) 6

Ex Parte Jackson,
96 U.S. 727 (1878) 3, 8, 9

Horton v. California,
496 U.S. 128 (1990) 9

Illinois v. Caballes,
543 U.S. 405 (2005) 15

Illinois v. Lafayette,
462 U.S. 640 (1983) 7

Katz v. United States,
389 U.S. 347 (1967) 2, 8, 12, 13

Kyllo v. United States,
533 U.S. 27 (2001) ..... *passim*

Los Angeles v. Patel,
576 U.S. ___ (2015) 17

Olmstead v. United States,
277 U.S. 438 (1928) 8, 10, 11

Riley v. California,
134 S. Ct. 2473 (2014) 3, 6, 7, 22

Smith v. Maryland,
442 U.S. 735 (1979) 14

South Dakota v. Opperman,
428 U.S. 364 (1976) 6

Terry v. Ohio,
392 U.S. 1 (1968) 5

United States v. Carpenter,
819 F.3d 880 (6th Cir. 2016) ..... *passim*

United States v. Jacobsen,
466 U.S. 109 (1984) 15

United States v. Jones,
132 S. Ct. 945 (2012) ..... *passim*

United States v. Miller,
425 U.S. 435 (1976) 16, 17

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 22

Constitutional Provisions

U.S. Const., amend. IV 2, 4

Statutes

12 U.S.C. § 1829b(a)(2) (2000) 16

18 U.S.C. §2703(d) 19

The Bank Secrecy Act, Pub. L. No. 91-508,
84 Stat. 1114 (codified as amended at
12 U.S.C. §§ 1951–59 (2000)) 16

Other Authorities

Gerald W. Brock, *The Second Information Revolution* (2003) 10

Jim Harper, *Escaping Fourth Amendment Doctrine After Jones: Physics, Law, and Privacy Protection*, 2012 Cato Sup. Ct. L. Rev. 219 9

Mark Taticchi, *Note: Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures*, 78 Geo. Wash. L. Rev. 476 (2010) 20

Orin Kerr, *Katz* Has Only One Step: The Irrelevance of Subjective Expectations, 82 U. Chi. L. Rev. 113 (2015) 13

Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005) 11, 21

Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85 (2014) 23

INTEREST OF *AMICUS CURIAE*[1]

The Cato Institute was established in 1977 as a nonpartisan public policy research foundation dedicated to advancing the principles of individual liberty, free markets, and limited government. Cato's Center for Constitutional Studies was established in 1989 to promote the principles of limited constitutional government that are the foundation of liberty. To those ends, Cato publishes books and studies, conducts conferences, produces the annual *Cato Supreme Court Review*, and files *amicus* briefs. The present case centrally concerns Cato because it represents an opportunity to improve Fourth Amendment doctrine and maintain that provision's protections in the modern era.

INTRODUCTION AND SUMMARY OF ARGUMENT

Timothy Ivory Carpenter and Timothy Michael Sanders were convicted in the U.S. District Court for the Eastern District of Michigan at Detroit on charges stemming from a string of armed robberies in and around the Detroit area. They appealed on the ground that the government had acquired detailed records of their movements from their wireless carriers in violation of the Fourth Amendment. The U.S. Court of Appeals for the Sixth Circuit turned their appeal aside, finding that "[t]he government's collection of business records containing these data ... is

---

[1] Rule 37 statement: All parties received timely notice of our intent to file and consented to the filing of this brief. No counsel for any party authored any of this brief and *amicus* alone funded its preparation and submission.

not a search." *United States v. Carpenter*, 819 F.3d 880, 887 (6th Cir. 2016).

In natural language and ordinary reasoning, collecting business records using legal compulsion is rather obviously "not a search." It is a seizure, which may or may not be reasonable. But under current Fourth Amendment doctrine, "not a search" stands in for one of several potential conclusions: Maybe business records are not "papers or effects." Maybe such records are not the defendants' to keep from others' view. Or maybe it was reasonable to seize them under these circumstances. We do not know because Fourth Amendment doctrine has little reference to the terms of the amendment itself.

Nearly every aspect of the appeals court's decision is shot through with doctrinal oddities that hide the rationale, oddities that would befuddle an uninitiated lawyer or an ordinary American trying to learn how the Fourth Amendment's protections work. This is not the fault of the court below, but of that doctrine, which has grown up around the Fourth Amendment since *Katz v. United States*, 389 U.S. 347 (1967).

For the sake of righting courts' application of the Fourth Amendment, this Court should accept certiorari in this case and decide it using reasoning that eschews doctrine and hews more closely to the language and meaning of the Fourth Amendment.

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. Absent doctrine, courts would analyze the elements of this language as follows: Was there a search? Was there a seizure? Was any such

search or seizure of "their persons, houses, papers, [or] effects"? Was any such search or seizure reasonable?

Courts use this methodology in cases involving familiar physical objects. But in harder cases, such as those dealing with communications and data, courts labor under doctrine that calls for a two-part test: First, a court will determine (or, as often, presume) that a defendant expects privacy in some item or fact. Then the court must gamely feign knowledge of whether society as a whole deems that expectation reasonable.

In corollaries to the "reasonable expectation of privacy" test, courts find government agents' *highly directed examinations aimed at finding things* "not a search" because the examination technique is directed only toward finding contraband. And in cases like this one, courts dismiss the seizure of highly revealing information as "not a search" because it passed into the possession of a third party, even when that party was required by contract and regulation to maintain the confidentiality of the information for the individual.

Consistent with deep precedent such as *Ex Parte Jackson*, 96 U.S. 727 (1878), this Court's recent cases, from *Kyllo v. United States*, 533 U.S. 27 (2001), through *United States v. Jones*, 132 S. Ct. 945, 565 U.S. ___ (2012), to *Riley v. California*, 134 S. Ct. 2473, 573 U.S. ___ (2014), provide a framework for administering the Fourth Amendment in a more reliable and juridical way. It is a framework that this Court should now articulately apply to key cases, including this one dealing with data. In doing so, this Court can give courts below, law enforcement, the

bar, and American citizens clear signals about how to apply our fundamental law, the Constitution, as a law.

As the importance of communications and data grows in society, the imperative to straightforwardly address their constitutional status rises. Without breaking past precedents, this Court can revise Fourth Amendment practice and determine when and how communications and data fit into the Fourth Amendment's categories of protected things. Doing so would permit courts below to address seizures and searches of communications and data forthrightly, confidently assessing the reasonableness of such government action. This case is an excellent opportunity to do that.

ARGUMENT

I. THIS COURT SHOULD APPLY THE TERMS OF THE FOURTH AMENDMENT IN ALL FOURTH AMENDMENT CASES

The first phrase of the Fourth Amendment says, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const., amend. IV. Absent doctrine, courts would analyze its elements as follows: Was there a search? Was there a seizure? Was any search or seizure of "persons, houses, papers, [or] effects"? Was any such search or seizure reasonable?

If there was a search or seizure, if it was of protected things, and if it was unreasonable, then the right has been violated. That is how to administer the Fourth Amendment.

In cases dealing with familiar objects, this Court applies the Fourth Amendment consistent with the language of the law. It looks for seizures and searches of defendants' protected items, then assesses whether or not they were reasonable. (Seizures often precede searches, so reversing the order in which the Fourth Amendment lists them is sensible.)

In *Terry v. Ohio*, 392 U.S. 1 (1968), for example, this Court applied the Fourth Amendment soundly, creating a lasting and useful precedent. The government had urged the Court to place brief "stop and frisk" incidents like a pat-down outside the scope of the law, *id.* at 16 n.12., arguing that police behavior short of a "technical arrest" or a "full blown-search" did not implicate constitutional scrutiny. *Id.* at 19. This Court rejected the idea that there should be a fuzzy line dividing "stop and frisk" from "search and seizure."

Instead, this Court wrote with granular precision about the seizure, then the search, of Terry: "[T]here can be no question ... that Officer McFadden 'seized' petitioner and subjected him to a 'search' when he took hold of him and patted down the outer surfaces of his clothing." *Id.* One following the other, the seizure and search were reasonable and therefore constitutional.

Though Justice Douglas dissented from the ruling, he agreed that Terry was "seized" within the meaning of the Fourth Amendment. *Id.* at 35 (Douglas, J., dissenting). "I also agree," he wrote, "that frisking petitioner and his companions for guns was a 'search.'" *Id.*

Terry and its progeny demonstrated their value again in the recent *Riley* decision, 134 S. Ct. 2473 (2014). Note the half-dozen dogs that didn't bark—seizures and searches of familiar objects like cars and people, which are administered using direct application of the Fourth Amendment's terms rather than doctrine.

In *Riley*, Officer Charles Dunnigan pulled David Riley over, seizing him and his car consistent with the application of the Fourth Amendment to traffic stops in *Brendlin v. California*. 551 U.S. 249, 254–63 (2007).

Upon learning that Riley was driving with a suspended driver's license, Officer Dunnigan removed him from the car, continuing the original seizure of Riley with an additional legal basis for doing so: reasonable suspicion of another violation.

Officer Ruggiero prepared the car for impoundment, a further seizure, consistent with a policy that prevents suspended drivers from returning to, and continuing to operate, their vehicles. He began an "impound inventory search" of the car, as approved in *South Dakota v. Opperman*. 428 U.S. 364, 376 (1976).

That search turned up guns in the engine compartment of the car, so Officer Dunnigan placed Riley under arrest, continuing the ongoing seizure of Riley's body under new legal authority.

Officer Dunnigan then conducted a search incident to arrest—permitted to aid in the discovery of weapons or of evidence that suspects might destroy. *Chimel v. California*, 395 U.S. 752, 762–63 (1969).

Consistent with standard practice for a "booking search," yet another legal basis for both searching

suspects and seizing their property, *see, e.g.*, *Illinois v. Lafayette*, 462 U.S. 640 (1983), Officer Dunnigan examined Riley's person and seized his possessions, including his cell phone.

All these government actions were unchallenged or fully disposed of in courts below because this Court has given law enforcement and courts the juridical tools to dispose of them: identify when seizures and searches have occurred, then determine whether or not they are reasonable.

Courts are well-equipped to make those legal and fact-specific judgments. If the constitutionality of all these investigatory steps turned on whether government agents had defeated a society-wide "reasonable expectation of privacy," this Court would have a full docket indeed.

Happily, *the Riley* opinion also assessed the search of the phone as the search that it was, without respect to privacy expectations. Having found that the phone was searched in the absence of exigency, this Court laid down the general rule of the second half of the Fourth Amendment: "get a warrant." 134 S. Ct. at 2495.

This Court does not need to retreat to doctrine when communications and data are at issue. These are items that can be seized and searched under the Fourth Amendment just like people and cars. Treating communications and data as such would focus courts on the key Fourth Amendment question: whether given seizures or searches are reasonable. Confusing doctrine stands in the way of them doing so.

II. THIS COURT SHOULD RETURN TO APPLYING THE TERMS OF THE FOURTH AMENDMENT IN COMMUNICATIONS AND DATA CASES, ESCHEWING THE UNSOUND "REASONABLE EXPECTATION OF PRIVACY" TEST

Relying on doctrine, the Sixth Circuit's decision below begins by noting an alleged constitutional distinction between communications content and routing information. "In Fourth Amendment cases the Supreme Court has long recognized a distinction between the content of a communication and the information necessary to convey it." *United States v. Carpenter*, 819 F.3d 880, 883 (6th Cir. 2016). An uninitiated lawyer or ordinary American would have difficulty understanding what this has to do with constitutional protection for "persons, houses, papers, and effects."

The appeals court begins as it does because in recent decades this Court has often fallen back on confusing doctrine when applying the Fourth Amendment in hard cases. But this Court can apply the terms of the Fourth Amendment to communications and data cases in a granular way, as it has in the past. A line of opinions from *Ex Parte Jackson*, 96 U.S. 727 (1878), through Justice Butler's dissent in *Olmstead v. United States*, 277 U.S. 438 (1928), and the majority opinion in *Katz v. United States*, 389 U.S. 347 (1967), show how to integrate communications and data with the Fourth Amendment's textual framework. But a detour over the last fifty years into "reasonable expectations" doctrine has undercut sound administration of the Fourth Amendment.

A. *Ex Parte Jackson* Protected Communications in Transit by Protecting Papers and Effects as Such

This Court correctly applied the Fourth Amendment to communications in *Ex Parte Jackson*, 96 U.S. 727 (1878). The opinion did not state in bullet-point order that the postal mail in question was a) searched, b) a paper or effect, and c) unreasonably searched without a warrant. But it held that "[l]etters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles." *Id.* at 733. Such things remain the papers and effects of their owners while in transit, and their contents are concealed, so searching them requires a warrant.

The outward form and weight of such items, not being sealed from inspection, are not constitutionally protected. This was early acknowledgement of the difference between plain view and what might be called "plain concealment." It takes no search to discover what is in plain view, so the Fourth Amendment is not implicated. *See Horton v. California*, 496 U.S. 128 (1990). It takes a search to reveal concealed matter, so the Fourth Amendment pertains. The issues are put in play by the Fourth Amendment's text and disposed of using physics and law, not privacy expectations. *See* Jim Harper, *Escaping Fourth Amendment Doctrine After* Jones*: Physics, Law, and Privacy Protection*, 2012 Cato Sup. Ct. L. Rev. 219.

In the current case, the court below, thrown off by doctrine in more recent cases, treated *Jackson* as a special rule about communications. 819 F.3d at 886.

But *Jackson* simply applied common sense: exposed facts do not require a search to be discovered, even when they are facts about papers and effects.

In the year this Court decided *Ex Parte Jackson*, both Western Union and the Bell Company began establishing voice telephone services, Gerald W. Brock, *The Second Information Revolution* 28 (2003). This Court would face that technology after the passage of some time, but perhaps before the properties of electronic communications were widely understood.

B. *Olmstead* Involved Seizures and Searches of a Wire and Electronic Papers/Effects

Fifty years later, the ruling in *Olmstead v. United States*, 277 U.S. 438 (1928), incoherently declared wiretapping "the use of the sense of hearing, and that only." *Id.* at 464. A telephone communication, of course, renders sounds as electronic signals that travel invisibly and inaudibly along a wire, to be reformed into audible sounds at the other end. Collecting those signals and reproducing them requires attachments, equipment, and information processing well beyond simple hearing.

Justice Butler's dissent stands out because he followed the same sensible lines drawn in *Jackson*, even though the medium was now wire and electrons instead of paper. Though he left implicit the physical protections for the communications, he identified the private law protections arrayed around telephone calls and the seizure and search that disrupts those arrangements when government agents wiretap a telephone line: "The contracts between telephone companies and users contemplate the private use of the facilities employed in the service," he wrote. "The

communications belong to the parties between whom they pass. During their transmission, the exclusive use of the wire belongs to the persons served by it." *Id.* at 487 (Butler, J., dissenting).

Government agents invaded property rights in the physical wire and in the communication running over it. Specifically, the government's use of the wire and copying of the electronic effects eviscerated Olmstead's right to exclude others from his property—a small but constitutionally significant seizure. The contemporaneous rendering of the communication signal into an audible sound was a search of it. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 551 (2005) ("[A] search occurs when information from or about the data is exposed to possible human observation . . . ."). The wiretap should have required a warrant.

It would have taken prescience indeed to recognize in the 1920s that telephonic and later digital communications would be the scions of physical mail. *But see, Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting) ("Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.") Even now, the idea that papers and effects may take electronic or digital form is a bit of a challenge. But that ground is long since broken. This Court's treated a suitably shrouded oral communication as a constitutionally protected item in 1967, and that result has been widely accepted, even if clarity as to the rationale for that finding still lacks.

C. The *Katz* Majority Inarticulately Applied the Fourth Amendment's Terms to a Shrouded Oral Communication

Regrettably when the Court reversed *Olmstead*, it avoided stating directly that the suitably concealed sound of a person's voice is a transitory "effect." (If the language of the Fourth Amendment applies, it almost certainly must be.) And even more unfortunately, the popular treatment of *Katz v. United States*, 389 U.S. 347 (1967), has been to ignore the majority's reasoning in favor of Justice Harlan's solo concurrence, which attempted to reframe the Court's Fourth Amendment jurisprudence around "reasonable expectations of privacy."

But the *Katz* majority decision was an inarticulate parallel to *Ex Parte Jackson*. The Court followed the same line as *Jackson* about disclosed matter requiring no search and concealed things requiring a seizure or search. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351 (citations omitted).

The paragraphs that followed discussed the import of Katz going into a phone booth made of glass, which concealed the sound of his voice. *Id.* at 352. Against the argument that Katz's body was in public for all to see, the Court wrote: "[W]hat he sought to exclude when he entered the booth was not the intruding eye– it was the uninvited ear." *Id.* The government's use of a secreted listening and recording device to enhance ordinary perception overcame the physical concealment Katz had given to his voice.

Gathering the sound waves seized something of Katz's.

But in his solo concurrence, which was unnecessary to the outcome of the case, Justice Harlan shared his sense of how the constitution controls government access to private communications: "My understanding," he wrote, "is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.* at 361. Justice Harlan's understanding has not aided courts' administration of cases.

D. The Ills of the "Reasonable Expectation of Privacy" Test

Since *Katz*, courts have often followed Justice Harlan's concurrence instead of the majority's rationale, attempting to analyze whether defendants have had a "reasonable expectation of privacy" in information or things. Under Harlan's concurrence, the defeat of a "reasonable expectation of privacy" signals a constitutional search generally requiring a warrant.

Alas, courts don't often follow the full analysis Justice Harlan's formulation suggests. They rarely inquire into a defendant's "actual (subjective) expectation of privacy," for example, or how it was "exhibited." *See* Orin Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. Chi. L. Rev. 113 (2015).

The second half of the test may flatter Justices and judges, who surely put care into their attempts to assess the entire society's emergent views on privacy, but it is a non-juridical methodology. It does not in-

volve the application of law to facts or fact-specific judgements. It requires judges to use their own views or best estimations about privacy as a proxy for objectivity.

A particularly poor example of the test in application is the opinion in *Smith v. Maryland*, 442 U.S. 735 (1979), in which Justice Blackmun walked through influences that would suppress expectations of privacy in phone-dialing information and none that would support it. *See id.* at 742–43. The court below in this case relied heavily on *Smith*, which in addition to being poorly reasoned may also be distinguished given the great quantities of data at stake in cases like this.

The slipperiness of Justice Harlan's formulation is compounded by its essential circularity. Societal expectations guide judicial rulings, which guide societal expectations, and so on. This circularity is especially problematic here at the onset of the Information Age because digital communications and data are only beginning to take their place in society. Expectations about privacy on this medium have yet to take form, and the technology continues to change, so there is simply no objectively reasonable sense of privacy for judges to discover.

E. Corollaries of the "Reasonable Expectation of Privacy" Test are Even Worse

The "reasonable expectation of privacy" test has at least two corollaries that move doctrine even further from the Fourth Amendment's language and meaning. The first is the doctrine that treats searches tailored for illegal things as non-searches. The second is

the "third-party doctrine," which denies that shared things can be unreasonably seized or searched.

Illinois v. Caballes, 543 U.S. 405 (2005), is typical of "reasonable expectation" cases in that it did not examine (or even assume) whether Roy Caballes had exhibited a subjective expectation of privacy in the trunk of his car, which government agents subjected to the ministrations of a drug-sniffing dog. Thus, the Court could not take the second step, examining its objective reasonableness.

Instead, the *Caballes* Court skipped forward to a corollary of the "reasonable expectations" test that the Court had drawn in *United States v. Jacobsen*, 466 U.S. 109 (1984): "Official conduct that does not 'compromise any legitimate interest in privacy' is not a search subject to the Fourth Amendment." *Caballes*, 543 U.S. at 408 (quoting *Jacobsen*, 466 U.S. at 123). Possession of drugs being illegal, there is no legitimate expectation of privacy in their possession. Thus, a search aimed at illegal drugs is not a search. That's confounding.

That entirely logical extension of "reasonable expectations" doctrine reveals the doctrine's role in delinking Fourth Amendment decisions from the Fourth Amendment's text. Now, instead of examining whether searches and seizures are reasonable, courts applying the *Jacobsen/Caballes* corollary can uphold any activity of government agents that appears sufficiently tailored to discovering only crime. The most *intensive government examination given to persons, houses, papers, and effects* can be "not a search," *id.*, no matter how intimate it is, no matter how often it recurs, and irrespective of any context or circumstances.

The second corollary of "reasonable expectations" doctrine, more relevant here, similarly breaks the link between the terms of the law and outcomes in cases. That is the "third party doctrine," which the court below relied on in this case.

The Bank Secrecy Act ("BSA"), Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 12 U.S.C. §§ 1951–59. (2000)) requires banks to maintain records and file reports with the Treasury Department if they "have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings." 12 U.S.C. § 1829b(a)(2) (2000).

In *California Bankers Association v. Shultz*, 416 U.S. 21 (1974), several parties challenged the BSA's requirements. The records-collection part of the law does not require disclosure to the government, so the Court found that it does not implicate the Fourth Amendment. *Id.* at 54. As to the reporting requirements, the Court denied standing to bank depositors who could not show that information about their financial transactions had been reported. *Id.* at 67–68.

Justice Marshall criticized how the Court avoided finding that mandated record-keeping affects a constitutional seizure just because the government would acquire the records later. "By accepting the Government's bifurcated approach to the recordkeeping requirement and the acquisition of the records, the majority engages in a hollow charade whereby Fourth Amendment claims are to be labeled premature until such time as they can be deemed too late." *Id.* at 97 (Marshall, J., dissenting).

Two years later, in *United States v. Miller*, 425 U.S. 435 (1976), the Court held that a defendant had

no Fourth Amendment interest in records maintained about him pursuant to the BSA. *Id.* at 442–43. It did not examine whether the operation of the BSA was a seizure or search, but used "reasonable expectations" doctrine to dismiss Miller's Fourth Amendment interests in documents reflecting his financial activities because they were held by a financial services provider: "we perceive no legitimate 'expectation of privacy' in their contents." *Id.* at 442.

Under these cases, the government can compel a service provider to maintain records about a customer and then collect those records without implicating his or her Fourth Amendment rights. *Cf. Los Angeles v. Patel*, 576 U.S. ___ (2015) (holding requirement that hotel operators make their guest registries available to the police on demand facially unconstitutional). The rule of *Miller* appears to be that Americans forfeit their Fourth Amendment interests in any material that comes into possession of a third party. This at least elides questions about who owns communications and data such as to enjoy a right to its protection from unreasonable seizure and search.

Based as they are in "reasonable expectations" doctrine, these holdings are hard to square with the Fourth Amendment's text. And they grow further out of synch with each step forward our society takes in modern, connected living.

Incredibly deep reservoirs of information are constantly collected by third-party service providers today. Cellular telephone networks pinpoint customers' locations throughout the day through the movement of their phones. Internet service providers maintain copies of huge swaths of the information that crosses their networks tied to customer identifiers. Search

engines maintain logs of searches that can be correlated to specific computers and the individuals that use them. Payment systems record each instance of commerce and the time and place it occurred.

The totality of these records are very, very revealing of innocent people's lives. They are a window onto each individual's spiritual nature, feelings, and intellect. They reflect each American's beliefs, thoughts, emotions, sensations, and relationships. Their security ought to be protected from unreasonable seizure, as they are the modern iteration of our papers and effects. *See United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). These items should generally not be seized without a warrant.

Thanks to recent cases, this Court is positioned to apply traditional legal concepts such as property rights to communications and data, placing them within the framework dictated by the text of the Fourth Amendment.

III. THIS COURT'S RECENT CASES ARE A FRAMEWORK FOR ADMINISTERING THE FOURTH AMENDMENT IN A RELIABLE AND JURIDICAL WAY

Familiar doctrine like the "reasonable expectation of privacy" test glosses over the challenges in integrating the Fourth Amendment's terms with the facts in particular cases. This Court's recent Fourth Amendment opinions, though, provide a framework for a clear return to adjudicating the Fourth Amendment as a law, even in difficult "high-tech" cases. In all cases, this Court can follow the methodology suggested by the Fourth Amendment, which is to look for searches, look for seizures, determine whether they

go to constitutionally protected items, and then determine whether they are reasonable.

This does not mean that the precise way to apply basic Fourth Amendment concepts to communications and data is already obvious. But carefully integrating long-standing legal principles with advancing technologies will facilitate the application to modern problems of Fourth Amendment concepts such as "seizure", "search", "papers", and "effects."

A. *Jones* was a Seizure Case

Though this Court referred to the totality of the disputed government action in *United States v. Jones*, 132 S. Ct. 945 (2012), as a "search," the precipitating constitutional invasion was a seizure. That seizure occurred when government agents attached a device to a car that was not theirs, making use of the car to transport their device, without a warrant. *Id.* at 949; *see ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (referring to attachment of GPS device in *Jones* as "a technical trespass on the defendant's vehicle"). Though small, that seizure of Jones's car, in the form of "use," was a sufficient trigger of scrutiny for constitutional reasonableness. It facilitated a weeks-long, contemporaneous search for Jones's location. Considering the outsized effect on Jones, who was still presumed innocent, the seizure and the search were unreasonable without a warrant.

The present case is a much simpler seizure case. The government here seized data under authority given by 18 U.S.C. §2703(d). *United States v. Carpenter*, 819 F.3d 880, 884 (6th Cir. 2016). When government agents copy data or information that is otherwise unavailable to them, they have taken the rights

to use the data and to enjoy that data's benefits for the government. The owner still has possession of a copy, but the owner's right to exclude others has been eviscerated. *See* Mark Taticchi, *Note: Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures*, 78 Geo. Wash. L. Rev. 476, 491–96 (2010). Through this case, this Court should recognize data as something that can be seized.

Is it a "paper" or "effect"? Is it the defendant's paper or effect in which to assert a right? These questions come later in a methodical analysis.

B. *Kyllo* is a Modern Search Case

Though less relevant here, this Court's opinion in *Kyllo v. United States*, 533 U.S. 27 (2001), is a wonderfully instructive modern "search" case, because it features search in the absence of seizure. That allows us to observe search in the abstract and see how concealment subjected to search produces exposure. Manufactured exposure of concealed things is a strong signal that a search has occurred.

The thermal-imaging cameras government agents used in *Kyllo* detect radiation in the infrared range of the electromagnetic spectrum (that is, with longer wavelengths than visible light). They produce images of that radiation called thermograms by representing otherwise invisible radiation in the visible spectrum. This makes imperceptible radiation perceptible to humans.

Using a thermal imager on a house was a search of it, and this Court found it so. "Where, as here, the Government uses a device that is not in general public use, to explore details of the home that

would previously have been unknowable without physical intrusion," the Court held, "the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Kyllo*, 533 U.S. at 40. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 553 ("For the holding in *Kyllo* to make sense, it must be the transformation of the existing signal into a form that communicates information to a person that constitutes the search. What made the conduct in *Kyllo* a search was not the existence of the radiation signal in the air, but the output of the thermal image machine and what it exposed to human observation.").

C. "Their Persons, Houses, Papers, and Effects"

This Court has been good to bestow relatively clear signals that items under consideration are within the categories listed for protection in the Fourth Amendment. In other cases, it is an essential premise of the Court's rulings. But the best practice would be to consistently and systematically recite each element of the Fourth Amendment as a model for lower courts.

The categorization of digital materials as paper, effects, or otherwise is a question that would benefit from sharpening by this Court in this case, as well as the ownership status of such items. The possessive pronoun in the Fourth Amendment circumscribes what items a defendant may assert Fourth Amendment interests in.

Pleasingly, the *Jones* Court declared the existence of a constitutionally protected item: "It is beyond dispute that a vehicle is an 'effect' as that term is used in the Amendment." 132 S. Ct. at 949. And it carefully detailed the ownership question, finding that Jones "had at least the property rights of a bailee." *Id.* at 949 n.2.

Riley, of course, dealt with the search of a cell phone. It is an essential premise of the ruling that phones themselves are effects. Dictum in *Riley* suggests that digital files are also effects.

The *Riley* Court declined the government's invitation to allow cell-phone searches if it is reasonable to believe that a phone contains evidence of the crime of arrest. 134 S. Ct. at 2492. Doing so, the Court said, would "in effect give police officers unbridled discretion to rummage at will among a person's private effects." *Id.* (quotation and citation omitted). This Court treated not just phones, but the digital documents and materials they hold, as effects.

The Sixth Circuit has found constitutional protection for emails, which also must rest on the premise that digital data in the form of an email file is a "paper" or "effect" for Fourth Amendment purposes. In *United States v. Warshak*, that court said: "Given the fundamental similarities between email and traditional forms of communications, it would defy common sense to afford emails lesser Fourth Amendment protection. Email is the technological scion of tangible mail." 631 F.3d 266, 285–86 (6th Cir. 2010).

The parallel between emails and tangible mail is the beginning but not the end of the relationship between digital files and the papers and effects categories. Again, the Fourth Amendment does not have special rules for communications, but covers all papers and effects equally. Email is but one of many protocols that replicate and expand on people's ability to collect, store, and transmit personal information as they did in the founding era. This court would best treat digital files as papers or effects, regardless of its determinations about the ownership status and reasonableness of seizing and searching particular files in any given case. The coverage of the Fourth Amendment must extend to these media if this Court is to succeed in "assuring preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34; *United States v. Jones*, 565 U.S. at 950; *id.* at 958 (Alito, J., concurring).

The final question before assessing the reasonableness of government action is whether a constitutionally protected item is the defendant's. Just as with telephones according to Justice Butler's view in *Olmstead*, people use modern communications and Internet facilities under contracts that allocate property rights. Though hardly with perfect clarity, these contracts detail how communications machinery will be used, and they divide up the ownership of information and data. *See*, Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85, 142–45 (2014). The regulatory regime for the telecommunications sector also arguably accords property rights in communications and data to the consumer-user.

The court below, applying doctrine, back-handedly dismissed this crucial question: whether the defendants had a property right in the data about them that the government seized. *United States v. Carpenter*, 819 F.3d 880, 887 (6th Cir. 2016) ("The defendants of course lack any property interest in cell-site records..."). This Court should take up this case in order to reinforce the importance of property principles for administering the Fourth Amendment—it lists items of property, after all—and to model for lower courts how this is done with care.

CONCLUSION

The analytical framework suggested above tees up the issue that is the central focus of the Fourth Amendment. That is the reasonableness of government agents in searching or seizing particular items.

There are very good arguments that communications, data, and data about communications are seized when government agents take them by compulsory processes. There are good arguments that these things are papers or effects for constitutional purposes. And there are arguments that the defendants, like all Americans, have property rights in such data, which is allocated to them by contract and regulation.

This Court should grant certiorari in this case to examine these arguments. The Court should sharpen its own application of the Fourth Amendment and provide a model for lower courts by eschewing "reasonable expectation of privacy" doctrine and by applying the terms of our fundamental law directly.

Respectfully submitted,

Jim Harper
Counsel of Record
Ilya Shapiro
CATO INSTITUTE
1000 Mass. Ave. N.W.
Washington, D.C. 20001
(202) 842-0200
jharper@cato.org

October 28, 2016

RECORD AND BRIEFS

Supreme Court, U.S.
FILED
AUG 11 2017
OFFICE OF THE CLERK

No. 16-402

IN THE
Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

BRIEF OF AMICI CURIAE DATA & SOCIETY RESEARCH INSTITUTE AND FIFTEEN SCHOLARS OF TECHNOLOGY AND SOCIETY IN SUPPORT OF PETITIONER

MARCIA HOFMANN
KENDRA ALBERT
ZEITGEIST LAW PC
25 Taylor St.
San Francisco, CA 94102

ANDREW D. SELBST
Counsel of Record
DATA & SOCIETY
RESEARCH INSTITUTE
36 W. 20th St., 11th Floor
New York, NY 10011
(617) 504-1982
andrew@datasociety.net

Attorneys for Amici Curiae

RECORD AND BRIEFS

No. 16-402

Supreme Court, U.S.
FILED
OCT 28 2016
OFFICE OF THE CLERK

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, BRENNAN CENTER FOR JUSTICE, CENTER FOR DEMOCRACY & TECHNOLOGY, THE CONSTITUTION PROJECT, AND NATIONAL COALITION TO PROTECT CIVIL FREEDOMS IN SUPPORT OF PETITIONER

RACHEL LEVINSON-WALDMAN
MICHAEL W. PRICE
BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
161 Avenue of the Americas,
12th Floor
New York, New York 10013
(646) 292-8335

JENNIFER LYNCH
Counsel of Record
ANDREW CROCKER
JAMIE WILLIAMS
STEPHANIE LACAMBRA
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
jlynch@eff.org

Attorneys for Amici Curiae

268699

Library of Congress

TABLE OF CONTENTS

Page

TABLE OF CONTENTS i

TABLE OF CITED AUTHORITIES iii

STATEMENT OF INTEREST 1

INTRODUCTION 1

ARGUMENT 3

I. The Dramatic Increase in Location Data Generated by Cell Phones, Collected by Third Parties and Available to Law Enforcement, Counsels in Favor of *Certiorari* 4

A. The Number of Cell Phones and Cell Sites Has Increased Significantly in the Last Thirty Years 4

B. As the Number of Cell Towers and Amount of Data Transmitted Increases, the Location Data Generated by Cell Phones Becomes Increasingly More Detailed 9

C. Law Enforcement Routinely Requests Access to Months of CSLI Without a Warrant 12

Table of Contents

Page

II. CSLI Paints a Revealing Portrait of a Person's Movements, Presenting Even Greater Privacy Concerns Than the GPS Tracker at Issue in *Jones* 14

III. Courts Have Misapplied *Smith v. Maryland* to Bar Fourth Amendment Protection for CSLI 17

A. Courts and Judges Disagree on the Application of the "Third-Party Doctrine" to CSLI 18

B. Users Do Not "Voluntarily Convey" CSLI to Providers 20

C. The Fourth Amendment Protects Sensitive Information Even if People Know a Third Party May Access It 22

D. Americans Reasonably Expect Location Data to Remain Private 23

CONCLUSION 26

APPENDIX 1a

TABLE OF CITED AUTHORITIES

Page

CASES

Bond v. United States,
529 U.S. 334 (2000). 22

City of Ontario v. Quon,
560 U.S. 746 (2010) 22, 23

Commonwealth v. Augustine,
4 N.E.3d 846 (Mass. 2014). 17, 19, 21

Ferguson v. City of Charleston,
532 U.S. 67 (2001). 22

Heffron v. International Society for Krishna Consciousness,
452 U.S. 640 (1981). 18

In Matter of United States,
40 F. Supp. 3d 89 (D.D.C. 2014). 19

In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.,
396 F. Supp. 2d 747 (S.D. Tex. 2005) 14-15, 21

In re Application for Tel. Info. Needed for a Criminal Investigation,
119 F. Supp. 3d 1011 (N.D. Cal. 2015). 9, 21

Cited Authorities

Page

In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device,
396 F. Supp. 2d 294 (E.D.N.Y. 2005) 19

In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.,
809 F.Supp.2d 113 (E.D.N.Y. 2011).....16, 19, 20

In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't,
620 F.3d 304 (3d Cir. 2010) 18, 21

In re Application of U.S. for Historical Cell Site Data,
724 F.3d 600 (5th Cir. 2013).....9, 18

In re Application of U.S.,
736 F. Supp. 2d 578 (E.D.N.Y. 2010),
rev'd (Nov. 29, 2010) 19

In re Application of U.S.,
Nos. 1:06–MC–6, 1:06–MC–7, 2006 WL 1876847
(N.D. Ind. July 5, 2006) 19

Kyllo v. United States,
533 U.S. 27 (2001).....17

Cited Authorities

Page

NAACP v. Alabama,
357 U.S. 449 (1958) 16

Oliver v. United States,
466 U.S. 170 (1984) 23

Riley v. California,
134 S.Ct. 2473 (2014) 1, 4, 15, 22

Roberts v. U.S. Jaycees,
468 U.S. 609 (1984) 16

Smith v. Maryland,
442 U.S. 735 (1979) ..... *passim*

State v. Earls,
70 A.3d 630 (N.J. 2013) 20

Stoner v. California,
376 U.S. 483 (1963) 22-23

Tracey v. State,
152 So. 3d 504 (Fla. 2014) 10, 19, 20, 21

Turner v. Rogers,
131 S. Ct. 2507 (2011) 19

U.S. v. Alvarez,
No. 14-CR-00120-EMC, 2016 WL 3163005
(N.D. Cal. June 3, 2016) 19

Cited Authorities

Page

U.S. v. Cooper,
No. 13–693, 2015 WL 881578
(N.D. Cal. Mar. 2, 2015) 19

United States v. Carpenter,
819 F.3d 880 (6th Cir. 2016) ..... *passim*

United States v. Davis,
754 F.3d 1205 (11th Cir. 2014) 18

United States v. Davis,
785 F.3d 498 (11th Cir. 2015) ..... *passim*

United States v. Graham,
796 F.3d 332 (4th Cir. 2015) ..... *passim*

United States v. Graham,
824 F.3d 421 (4th Cir. 2016) ..... *passim*

United States v. Graham,
846 F. Supp. 2d 384 (D. Md. 2012) 19

United States v. Jones,
132 S. Ct. 945 (2012) ..... *passim*

United States v. Jones,
908 F. Supp. 2d 203 (D.D.C. 2012) 16

United States v. Thomas,
No. 3:15CR80, 2015 WL 5999313
(E.D. Va. Oct. 13, 2015) 19

Cited Authorities

Page

STATUTES

18 U.S.C. § 2703(d) 14

18 U.S.C. §§ 2701–2712 5

OTHER AUTHORITIES

Monica Anderson, *6 Facts About Americans and Their Smartphones*, Pew Research Center (Apr. 1, 2015) 7

AntennaSearch.com 6, 11, 12

AT&T, *AT&T Transparency Report* (2016) 12

Jan Lauren Boyles, et al., *Privacy and Data Management on Mobile Devices*, Pew Research Internet & American Life Project (Sept. 5, 2012) 24

CTIA—The Wireless Association, *Annual Year-End 2015 Top-Line Survey Results* (May 2016) 5, 6, 7, 8

David Deasy, *TRUSTe Study Reveals Smartphone Users More Concerned About Mobile Privacy Than Brand or Screen Size*, TRUSTe Blog (Sept. 5, 2013) 25

Jesus Diaz, *How Large Is a Petabyte?*, Gizmodo (July 8, 2009) 8

Cited Authorities

Page

Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. (2011) 9

Harris Interactive, *2013 Mobile Consumer Habits Study* (June 2013) 4

Letter from Timothy P. McKone, Executive Vice President, AT&T, to Rep. Edward J. Markey (Oct. 3, 2013).....10

Mary Madden, et al., *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Center (Nov. 12, 2014).....24

Lee Rainie, *Cell Phone Ownership Hits 91% of Adults*, Pew Research Center (June 6, 2013).....4

Marguerite Reardon, *Cell Phone Industry Celebrates Its 25th Birthday*, CNET (Oct. 13, 2008) 4

Sprint, *Sprint Corporation Transparency Report* (July 2016) 13

Bennett Stein, ACLU, *Fighting a Striking Case of Warrantless Cell Phone Tracking* (July 1, 2013) 15

T-Mobile Transparency Report (2013-2014) 13

Cited Authorities

Page

Abigail Tracy, *T-Mobile Leads US Wireless Carriers In Government Data Requests*, Forbes (July 6, 2015) 13

Janice Y. Tsai, *et al.*, *Location-Sharing Technologies: Privacy Risks and Controls*, Carnegie Mellon University (Feb. 2010) 25

U.S. Census Bureau, *U.S. and World Population Clock* 5

Verizon, *2015 (1st Half) Transparency Report* 13

Verizon, *2015 (2nd Half) Transparency Report* 13

Verizon, *Verizon's Transparency Report for the First Half of 2016: U.S. Report* (2016) 13, 16

Kathryn Zickuhr, *Location-Based Services*, Pew Research Internet & American Life Project (Sept. 12, 2013) 24

CONSTITUTIONAL PROVISIONS

U.S. Const., amend IV ..... *passim*

U.S. Const., amend. I 16

Cited Authorities

Page

LEGISLATIVE AUTHORITIES

Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance, Hearing Before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations, of the H. Comm. on the Judiciary, 113th Cong. 50 (2013) (written testimony of Professor Matt Blaze, University of Pennsylvania) 6, 8, 10, 11

STATEMENT OF INTEREST[1]

Amici are organizations committed to ensuring constitutional rights continue to be protected as technology advances and include the Electronic Frontier Foundation, the Brennan Center for Justice at NYU School of Law, the Center for Democracy & Technology, the Constitution Project, and the National Coalition to Protect Civil Freedoms. Many of these organizations have appeared previously as *amicus curiae* before this Court. Their individual organizational statements are contained in the Appendix following this brief.

INTRODUCTION

Cell phones have become "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 134 S.Ct. 2473, 2484 (2014). In *Riley*, this Court recognized that the ubiquity of cell phones, combined with their capacity to hold vast quantities of detailed personal information—potentially the "sum of an individual's private life"—makes cell phones so qualitatively and quantitatively different from their analog counterparts as to require a warrant prior to search. *Id.* at 2489.

---

1. Pursuant to Supreme Court Rule 37.2(a), *amici* have provided timely notice to all counsel, and all parties consent to the filing of this brief. Pursuant to Supreme Court Rule 37.6, *amici* state this brief was not authored in whole or in part by counsel for any party, and that no person or entity other than *amici* or their counsel made a monetary contribution to fund the preparation or filing of this brief.

However, the private information available from cell phones is not limited to the data stored on the phone itself. For a phone to receive and share much of that data—in other words, to be usable—it must connect with a cell tower. Every time it does, it generates information, stored by the phone company, about which tower the phone connected to—essentially where the phone was—on a given date and time. These small bits of data—called cell site location information (CSLI)—are aggregated by providers and, like GPS data that may be stored on the phone itself, "generate[] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *United States v. Jones*, 132 S.Ct. 945, 955 (2012) (Sotomayor, J., concurring).

CSLI is proving increasingly useful to law enforcement. As cell phone use has increased, so too has the number of cell towers or cell "sites," leading to increasingly precise location information on individuals. Equipped with CSLI, police can now not only place suspects at specific crime scenes, but can also reconstruct almost anyone's movements for many months in the past.

The petitions for *certiorari* in *Graham v. United States*, Case No. 16-6308, and *Carpenter v. United States*, Case No. 16-402,[2] ask this Court to address whether the Fourth Amendment prohibits the warrantless seizure and search of CSLI. Both cases relied on this Court's opinion in *Smith v. Maryland*, 442 U.S. 735 (1979), to hold Americans lack a reasonable expectation of privacy in CSLI because it is a business record held by third-party

2. *Amici* believe the issues raised by both cases are substantially similar and have filed the same brief in support of both petitions for *certiorari*.

service providers. But the few days of numbers dialed in *Smith* are so qualitatively different from the months of detailed location data collected in these cases as to prove Justice Sotomayor's point that *Smith's* premise is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 132 S.Ct. at 957 (Sotomayor, J. concurring).

As CSLI has become more precise and revealing, and as law enforcement increasingly relies on this data to secure criminal convictions, the time is ripe for this Court to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Id.* The Court should grant *certiorari* to address this issue and make clear that the Fourth Amendment requires a warrant for CSLI.

ARGUMENT[3]

Americans carry their cell phones with them everywhere and, as they do, they generate increasingly granular and detailed information about where they have been and when. This data is purely a byproduct of owning and carrying an operational phone—it is created whenever the phone tries to send and receive information, generally without forethought or conscious action by the owner. And it is stored with third-party service providers who may retain it for years.

The dramatic increase in the number of cell phones and cell sites and the amount of detailed, sensitive location

3. Except where noted, all cited web sites were last visited on October 20, 2016.

data they generate, combined with the quantity and extent of law enforcement demands for this data, show that it is time for this Court to address the Fourth Amendment privacy implications of CSLI. The fact that judges within the federal and state court systems are in stark disagreement regarding whether a warrant is required to obtain this data only underscores this point.

I. The Dramatic Increase in Location Data Generated by Cell Phones, Collected by Third Parties and Available to Law Enforcement, Counsels in Favor of *Certiorari*

A. The Number of Cell Phones and Cell Sites Has Increased Significantly in the Last Thirty Years

As in *Riley*, the "element of pervasiveness that characterizes cell phones" has a crucial impact on the Fourth Amendment issues here. *Riley*, 134 S.Ct. at 2490. Today, owning a cell phone is not a luxury; more than 91% of all American adults have a cell phone, and most carry their phone with them everywhere they go.[4]

The first commercial cell phone service was offered in the United States in 1983[5]—four years after this Court's

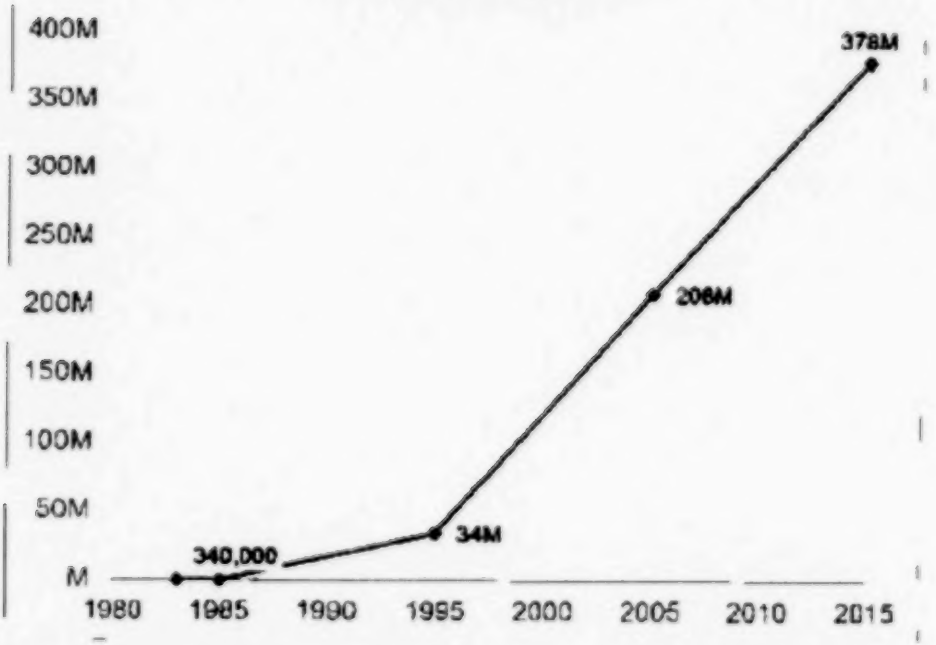
---

4. *See* Lee Rainie, *Cell Phone Ownership Hits 91% of Adults*, Pew Research Center (June 6, 2013), http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/; Harris Interactive, *2013 Mobile Consumer Habits Study* 2 -3 (June 2013), *available at* http://pages.jumio.com/rs/jumio/images/Jumio%20-%20Mobile%20Consumer%20Habits%20Study-2.pdf.

5. Marguerite Reardon, *Cell Phone Industry Celebrates Its 25th Birthday*, CNET (Oct. 13, 2008), https://www.cnet.com/news/cell-phone-industry-celebrates-its-25th-birthday.

seminal decision in *Smith v. Maryland* and three years before Congress enacted the Stored Communications Act ("SCA"), 18 U.S.C. §§2701–2712. Since that time, the number of mobile device accounts in the United States has grown to an estimated 378 million—53 million more accounts than people.[6]

Chart 1: Number of Mobile Device Subscriptions in United States[7]



6. CTIA—The Wireless Association, *Annual Year-End 2015 Top-Line Survey Results* 3 (May 2016) ("CTIA 2015 Survey"), *available at* http://www.ctia.org/docs/default-source/default-document-library/ctia-survey-2015.pdf (378 million mobile device accounts); *see* U.S. Census Bureau, *U.S. and World Population Clock*, http://www.census.gov/popclock (estimated U.S. population 325 million on October 5, 2016).

7. Charts 1–3 were generated using statistics from an annual survey of wireless service providers conducted by CTIA-The Wireless Association, the leading wireless industry trade association. *See* CTIA 2015 Survey at 3.

Cell phones send and receive radio signals via base stations, known as cell towers. Towers typically have multiple cell "sites" facing in three or four different directions, each containing antennae that detect radio signals emanating from phones and that connect the phones to the cellular network.[8] Cell phones automatically try to connect to the nearest or strongest base station, and, as users move farther away from one base station and closer to another, their phones automatically transfer the connection to the new base station.

As cell phone use has increased, service providers have installed more cell sites to handle the load.[9] Estimates of the current number of cell sites in the United States range from 300,000 to 600,000.[10] These sites include an estimated 1.85 million antennae, constantly communicating with all phones in range.[11]

---

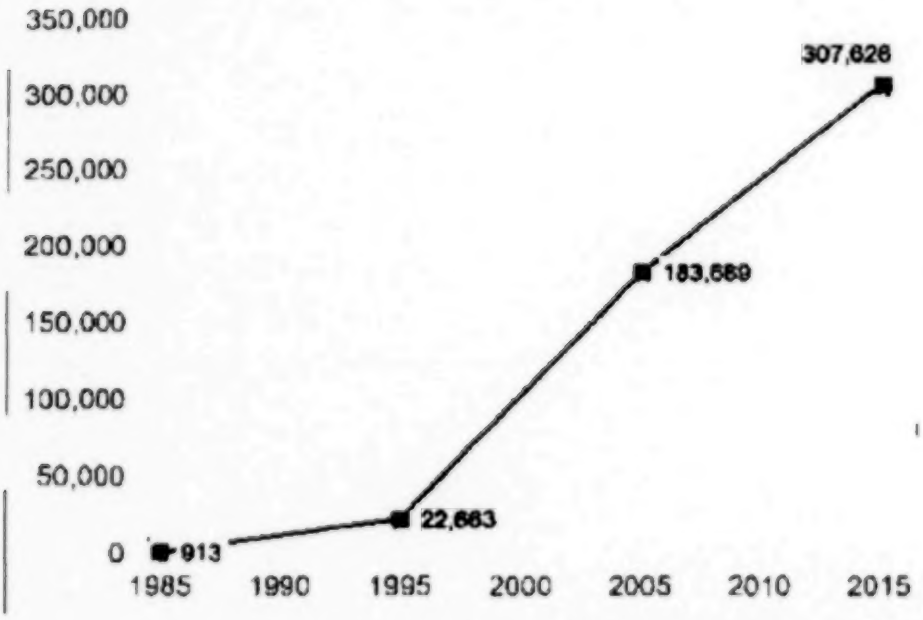
8. *See* Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance, Hearing Before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations, of the H. Comm. on the Judiciary, 113th Cong. 50, at 6, 9 (2013) (written testimony of Professor Matt Blaze, University of Pennsylvania) ("Blaze Testimony"), *available at* https://judiciary.house.gov/wp-content/uploads/2016/02/Blaze-Testimony.pdf.

9. Blaze Testimony at 10 ("A sector base station can handle only a limited number of simultaneous call connections given the amount of radio spectrum 'bandwidth' allocated to the wireless carrier.").

10. CTIA 2015 Survey at 2 (307,626 cell sites in 2015); AntennaSearch.com, http://antennasearch.com (618,950 cell towers as of Oct. 2, 2016).

11. AntennaSearch.com, http://antennasearch.com (1,852,945 antennas as of Oct. 2, 2016).

Chart 2: Number of Cell Sites in United States[12]



Modern cell phones' increasing sophistication and improved capabilities have also driven the need for more cell sites. After Apple released the iPhone in 2007, "smartphones" took off. Now more than 64% of Americans own smartphones.[13] For a significant percentage of "smartphone-dependent" Americans, their phones are their only means of accessing the Internet; this is disproportionately true for young adults, people of color, and lower-income Americans.[14]

---

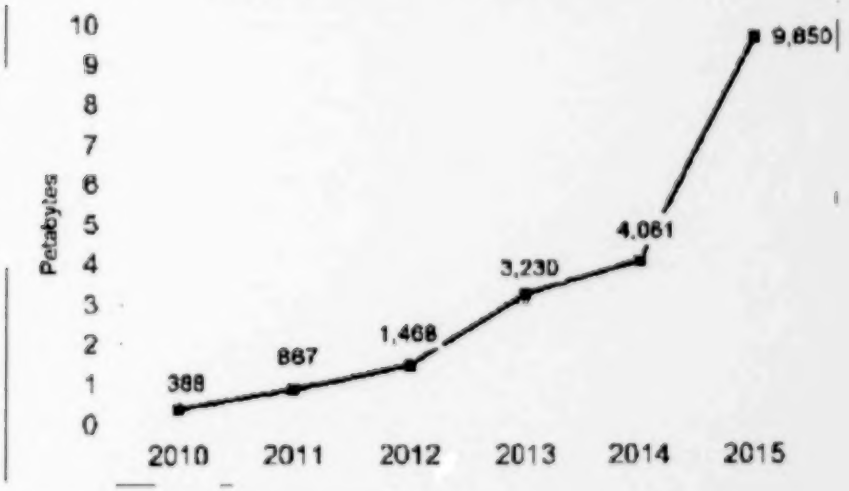
12. CTIA 2015 Survey at 2.

13. Monica Anderson, *6 Facts About Americans and Their Smartphones*, Pew Research Center (Apr. 1, 2015), http://www.pewresearch.org/fact-tank/2015/04/01/6-facts-about-americans-and-their-smartphones/.

14. *Id.* (noting the following percentages of "smartphone-dependent" Americans: 18-29 year olds (15%); adults with an annual household income of less than $30,000 (13%) versus adults with an income of $75,000 or above (1%); Latinos (13%) and African Americans (12%) versus whites (4%)).

Smartphones allow users to do everything from take and share photos, connect with friends through a variety of video and text-based communication tools, find the fastest route to a new location, stream music, research health information, play games, and track finances—and do all of these things at the same time. As a result, smartphones transmit and receive vast amounts of data. As more Americans have switched to smartphones, the amount of data transferred over wireless networks has increased significantly—2,400% between 2010 and 2015 alone[15]—and service providers have installed more towers to handle that increase.[16]

Chart 3: Wireless Data Traffic (in Petabytes)[17]



15. CTIA 2015 Survey at 8 (388 billion megabytes in 2010, 9,650 billion megabytes in 2015).

16. Blaze Testimony at 10.

17. CTIA 2015 Survey at 8. One source has described a petabyte of data as the equivalent of 20 million four-drawer filing cabinets filled with text. *See* Jesus Diaz, *How Large Is a Petabyte?*, Gizmodo (July 8, 2009), http://gizmodo.com/5309889/how-large-is-a-petabyte.

B. As the Number of Cell Towers and Amount of Data Transmitted Increases, the Location Data Generated by Cell Phones Becomes Increasingly More Detailed

When cell phones connect to cell sites, they generate CSLI—a record of the location of the cell tower the phone connected to at a specific moment in time. Modern cell phones—particularly smartphones—generate vast amounts of CSLI because they routinely send and receive data whenever the phone is on.

Cell phones generate CSLI even in the absence of any user interaction with the phone, in part due to "'applications that continually run in the background that send and receive data (*e.g.*, email applications) without a user having to interact with the cellular telephone.'" *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011, 1014 (N.D. Cal. 2015) ("*2015 N.D. Cal. Opinion*") (quoting Declaration of FBI Special Agent Hector M. Luna). Although some courts have limited their analysis of CSLI to data generated when users place and terminate a call,[18] the government has admitted it seeks access to CSLI generated by apps running in the background. *See id.* at 1033.

Cell phones connect with towers to exchange data on average every seven to nine minutes but can attempt to connect as frequently as every seven seconds.[19] Because

---

18. *See United States v. Davis*, 785 F.3d 498, 503 (11th Cir. 2015); *see also In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600, 615 (5th Cir. 2013) ("Fifth Circuit Opinion").

19. *2015 N.D. Cal. Opinion*, 119 F. Supp. 3d at 1028; Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681, 703 (2011).

these data exchanges create a record of when the user connected to the tower, along with the location of the tower itself, they reveal where the phone—and by proxy, its owner—has travelled. Cell providers store this data for up to five years[20] and can also track CSLI in near real-time.[21]

Law enforcement officers rely on CSLI to place a suspect at a specific location at a specific time, such as at the scene of a crime. *See, e.g., United States v. Carpenter*, 819 F.3d 880, 884 (6th Cir. 2016) (FBI used CSLI to place defendants to within 1/2 to 2 miles of robbery locations at times robberies occurred); *see also United States v. Graham*, 796 F.3d 332, 341 n.11 (4th Cir. 2015) (panel). In the past, CSLI was less accurate, because it consisted only of the location of the base station the phone connected to and the approximate "sector" served by that base station. Sectors could be several miles in diameter, so the phone could, theoretically, be anywhere within that area.

Now, however, CSLI has become much more detailed and specific. As the number of cell towers has increased and cell sites have become more concentrated, the geographic area covered by each cell sector has shrunk.[22] Cell phone triangulation (data from three towers instead of one), allows more precise location tracking, and with newer cell technology, providers can determine not just the location of the cell site the phone connects to, but, by

---

20. *See Letter from Timothy P. McKone, Executive Vice President, AT&T, to Rep. Edward J. Markey* 3 (Oct. 3, 2013), *available at* http://www.markey.senate.gov/imo/media/doc/2013-10-03_ATT_re_Carrier.pdf.

21. *See Tracey v. State*, 152 So. 3d 504, 507 (Fla. 2014).

22. Blaze Testimony at 10.

"correlating the precise time and angle at which a given device's signal arrives at multiple sector base stations," they can determine where the phone is located within a sector.[23] This can shrink accuracy down to within 50 meters.[24] Providers are also using small base stations designed to serve individual homes or offices, or even particular floors of buildings.[25] With these technologies, providers can determine "a phone's latitude and longitude at a level of accuracy that can approach that of GPS."[26]

These advances in cell service technology have especially impacted dense metropolitan areas with large numbers of mobile devices attempting to exchange data. For example, within two miles of the Supreme Court building, there are approximately 130 cell towers and 900 antennae.[27] In areas like these, the higher concentration of towers and antennae allow phones' locations to be pinpointed with even greater accuracy.

---

23. *Id.* at 12.

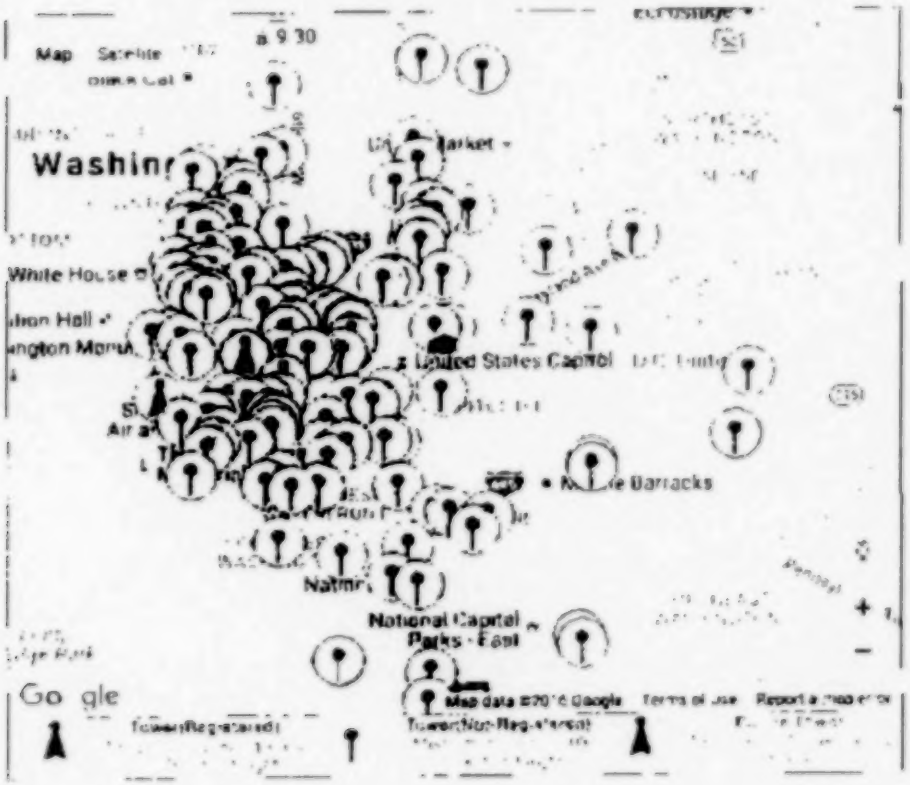
24. *Id.*

25. *Id.* at 11.

26. *Id.* at 12.

27. AntennaSearch.com, http://tinyurl.com/jgawkyp (tower search results); http://tinyurl.com/hkx4t4h (antenna search results).

Map of Cell Towers Within Two Miles of Supreme Court[28]



C. Law Enforcement Routinely Requests Access to Months of CSLI Without a Warrant

As cell phones saturate the country, law enforcement agencies routinely seek access to CSLI in criminal cases. The number of these requests is staggering. For example, AT&T alone received 36,935 requests for CSLI in the first half of 2016 and 76,340 requests in all of 2015.[29] Verizon

28. *Id.*

29. *See* AT&T, *AT&T Transparency Report* 4 (2016), *available at* http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_TransparencyReport_July2016.pdf (disclosing number of

received 24,928 requests in the first half of 2016 and 50,066 requests in 2015.[30] Sprint, the service provider in *Graham*, received 30,640 requests for real-time location data in the first half of 2016 and 64,854 requests in 2015.[31] *Graham*, 796 F.3d at 341 (panel). T-Mobile, the parent company of MetroPCS and the service provider in *Carpenter*, 819 F.3d at 885, does not report requests for CSLI specifically but received far more requests for customer data as a whole than its much larger rivals.[32]

As high as these numbers are, they do not tell the full story. Each request may seek information on many different phones. For example, in *Carpenter*, officers

---

requests for historical CSLI, real-time CSLI, and "cell tower dumps" – identifying information for all phones that connected to a tower during a given period of time).

30. *See* Verizon, *Verizon's Transparency Report for the First Half of 2016: U.S. Report* (2016), *available at* https://www.verizon.com/about/portal/transparency-report/us-report/; *see also* Verizon, *2015 (1st Half) Transparency Report* and Verizon, *2015 (2nd Half) Transparency Report*, *available at* https://www.verizon.com/about/portal/transparency-report/archive/ (numbers include "location information" and cell tower dumps).

31. Sprint, *Sprint Corporation Transparency Report* 4 (July 2016), *available at* http://goodworks.sprint.com/content/1022/files/Transaparency%20Report%20July2016.pdf (Sprint's report does not track other forms of location data).

32. Abigail Tracy, *T-Mobile Leads US Wireless Carriers In Government Data Requests*, Forbes (July 6, 2015), http://www.forbes.com/sites/abigailtracy/2015/07/06/t-mobile-leads-u-s-wireless-carriers-in-government-data-requests/#5cb644f54c88; *see also* T-Mobile, *T-Mobile Transparency Report* (2013-2014), *available at* https://newsroom.t-mobile.com/content/1020/files/NewTransparencyReport.pdf.

relied on three requests to access information about 16 different phones. 819 F.3d at 884. The quantity of data requested for each phone may vary as well. In *Graham*, with a single request, agents were able to obtain 221 days worth of location information for Mr. Graham and his co-defendant. 796 F.3d at 341 (panel). In *Carpenter*, the FBI obtained three to four months worth of data. 819 F.3d at 895 (Stranch, J., concurring).

The majority of these demands for CSLI are warrantless. Verizon has reported that two-thirds of all law enforcement requests for historical and real-time location information were made via a court order,[33] like the orders issued under 18 U.S.C. § 2703(d) that the government obtained in both *Carpenter* and *Graham*. *Carpenter*, 819 F.3d at 884; *Graham*, 796 F.3d at 344 (panel).

II. CSLI Paints a Revealing Portrait of a Person's Movements, Presenting Even Greater Privacy Concerns Than the GPS Tracker at Issue in *Jones*

The amount of CSLI generated as a result of society's reliance on cell phones means that law enforcement has access to an incredibly detailed picture of people's private lives and associations. *Jones*, 132 S.Ct. at 955 (Sotomayor, J., concurring). As noted in one of the first published opinions to address CSLI, the "combination of market and regulatory stimuli ensures that cell phone tracking will become more precise with each passing year." *In re*

---

33. *See* Verizon, *Verizon United States Report* (2016), *available at* https://www.verizon.com/about/portal/transparency-report/?page_id=2133.

Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 755 (S.D. Tex. 2005) ("*S.D. Tex. 2005 Opinion*").

Until the twenty-first century, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." *Jones*, 132 S.Ct. at 964 (Alito, J., concurring in the judgment). But CSLI has eviscerated that expectation and presents even greater privacy concerns than the GPS device this Court considered in *Jones*.

First, a GPS device attached to a car can only go where the car goes, while a cell phone goes everywhere its owner goes. As this Court noted in *Riley*, "three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting they even use their phones in the shower." 134 S.Ct. at 2490 (citations omitted). Therefore, as the panel noted in *Graham*, "unlike GPS monitoring of a vehicle, examination of historical CSLI can permit the government to track a person's movements between public and private spaces, impacting at once her interests in both the privacy of her movements and the privacy of her home." 796 F.3d at 348 (panel). And, in fact, using Mr. Graham's records, the ACLU was able to infer details about his patterns of movement, including when he and his pregnant wife visited her obstetrician, when he traveled to or from his home, and nights he spent away from home.[34]

---

34. *See* Bennett Stein, *Fighting a Striking Case of Warrantless Cell Phone Tracking*, ACLU (July 1, 2013), https://www.aclu.

Second, CSLI can give law enforcement far more information about a person's movements than the 28 days of monitoring that five members of this Court found problematic in *Jones*. *See* 132 S.Ct. at 964 (Alito, J., concurring in the judgment) (line at which tracking of vehicle became a search "was surely crossed before the 4-week mark"); *id.* at 955 (Sotomayor, J., concurring). The government obtained 88 days and 127 days worth of location information for each defendant in *Carpenter* and 221 days of data for each defendant in *Graham*. *Carpenter*, 819 F.3d at 886; *Graham*, 796 F.3d at 349 (panel). In other cases, the government has sought records for 67 days, 113 days, and 180 days. *Davis*, 785 F.3d at 501; *In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F.Supp.2d 113, 114 (E.D.N.Y. 2011) ("*2011 E.D.N.Y. Opinion*"); *United States v. Jones*, 908 F.Supp.2d 203, 206 (D.D.C. 2012). Because cell providers keep records of CSLI for up to five years, law enforcement officers could seek access to this data for even longer periods of time. Such extensive monitoring reveals a wealth of information about a person's expressive and associational activities protected by the First Amendment, in addition to the Fourth Amendment's protections against unreasonable searches. *See Smith*, 442 U.S. at 751 (Marshall, J. dissenting) (citing *NAACP v. Alabama*, 357 U.S. 449, 461 (1958)); *Roberts v. U.S. Jaycees*, 468 U.S. 609, 617-18 (1984).

Third, historical CSLI allows police to reconstruct a person's *past* movements. As Justice Alito noted in

---

org/blog/fighting-striking-case-warrantless-cell-phone-tracking (noting records were analyzed with Mr. Graham's "assistance and permission").

Jones, tracking a car's location for 28 days "would have [traditionally] required a large team of agents, multiple vehicles, and perhaps aerial assistance." 132 S.Ct. at 963 (Alito, J., concurring in the judgment). But CSLI allows police to go back in time to recreate a person's past movements, something not possible with the GPS tracker in *Jones* and *never* available through traditional law enforcement investigative techniques. *See Commonwealth v. Augustine*, 4 N.E.3d 846, 865 (Mass. 2014).

Finally, CSLI is generated for *all* phones, not simply those under investigation. Accordingly, unlike the GPS device in *Jones*, police need not even know in advance whether they want to track a particular individual. Rather, they have the ability to track nearly *any* person's location.

This Court has noted it is "foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001). With historical CSLI, the "practical" privacy protections of tracking a person's movement for months in the "pre-computer age"—namely difficulty and cost—have faded away. *Jones*, 132 S.Ct. at 963 (Alito, J., concurring in the judgment).

III. Courts Have Misapplied *Smith v. Maryland* to Bar Fourth Amendment Protection for CSLI

The majority opinions in *Carpenter* and *Graham* relied on this Court's decision in *Smith v. Maryland* to hold that the Fourth Amendment does not protect CSLI. *Smith* held that an individual has no reasonable expectation of privacy in the telephone numbers he dials because they

are business records that he "voluntarily conveyed" to the phone company. 442 U.S. at 744. But as other state and federal courts and judges have noted, *Smith* should not control here. Given "the important constitutional issues presented and the conflicting results reached" in CSLI cases, this Court should grant *certiorari* to clarify the scope of its prior rulings on the expectation of privacy in information shared with third parties. *Heffron v. International Society for Krishna Consciousness*, 452 U.S. 640, 646 (1981).

A. Courts and Judges Disagree on the Application of the "Third-Party Doctrine" to CSLI

In the roughly ten years that courts have been considering the Fourth Amendment's application to CSLI, there has been intense disagreement among judges and courts in both the state and federal systems. Within the five federal Circuit Courts of Appeal that have addressed the issue, many judges would hold or have held the third-party doctrine does not bar Fourth Amendment protection for CSLI.[35] In federal circuits where appellate courts have yet to address this issue—including the Second, Seventh, and Ninth Circuits—district court judges have also held

---

35. *See, e.g.*, *United States v. Graham*, 824 F.3d 421, 446 (4th Cir. 2016) (en banc) (Wynn, J., dissenting in part, joined by Floyd, J. and Thacker, J.); *Graham*, 796 F.3d at 354 (panel) (Davis, J., joined by Thacker, J.); *Carpenter*, 819 F.3d at 895 (Stranch, J., concurring); *Davis*, 785 F.3d at 535 (Martin, J., joined by Pryor, J., dissenting); *United States v. Davis*, 754 F.3d 1205, 1217 (11th Cir. 2014) (panel); *Fifth Circuit Opinion*, 724 F.3d at 615–16 (Dennis, J., dissenting); *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 317–18 (3d Cir. 2010) ("*Third Circuit Opinion*").

the third-party doctrine does not apply to CSLI.[36] Other federal judges have recognized the strong privacy interest in CSLI but concluded their hands were tied by *Smith*,[37] or simply acknowledged the need for further guidance from this Court.[38] As one court concluded after reviewing 87 CSLI opinions, "these decisions are impossible to reconcile." *In Matter of United States*, 40 F. Supp. 3d 89, 91 (D.D.C. 2014).

Graham and *Carpenter* are also in conflict with several state supreme court decisions, another factor weighing in favor of granting certiorari. *See Turner v. Rogers*, 131 S.Ct. 2507, 2514 (2011). The supreme courts of three states—New Jersey, Massachusetts, and Florida—have held that law enforcement needs a warrant to access at least some types of CSLI. *See Tracey*, 152 So. 3d 504 (Fla. 2014); *Augustine*, 4 N.E.3d 846 (Mass. 2014)

---

36. *See, e.g., 2011 E.D.N.Y. Opinion*, 809 F. Supp. 2d at 126; *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device*, 396 F. Supp. 2d 294, 322-23 (E.D.N.Y. 2005); *In re Application of U.S.*, Nos. 1:06-MC-6, 1:06-MC-7, 2006 WL 1876847, at *4 (N.D. Ind. July 5, 2006); *U.S. v. Alvarez*, No. 14-CR-00120-EMC, 2016 WL 3163005 *at 3 (N.D. Cal. June 3, 2016); *U.S. v. Cooper*, No. 13-693, 2015 WL 881578, at *7-8 (N.D. Cal. Mar. 2, 2015); *N.D. Cal. 2015 Opinion*, 119 F. Supp. 3d at 1027.

37. *See, e.g., United States v. Graham*, 846 F. Supp. 2d 384, 389-90, 394 (D. Md. 2012), *aff'd but criticized*, 796 F.3d 332 (4th Cir. 2015), *adhered to in part on reh'g en banc*, 824 F.3d 421 (4th Cir. 2016); *Davis*, 785 F.3d at 524 (Rosenbaum, J. concurring); *In re Application of U.S.*, 736 F. Supp. 2d 578, 589, n.12 (E.D.N.Y. 2010), rev'd (Nov. 29, 2010).

38. *See, e.g., United States v. Thomas*, No. 3:15CR80, 2015 WL 5999313, at *7 (E.D. Va. Oct. 13, 2015).

(deciding case under the state constitution); *State v. Earls*, 70 A.3d 630 (N.J. 2013) (same). As the Florida Supreme Court recognized, "cumulative cell-site-location records implicate sufficiently serious protected privacy concerns" and cell-phone users have a reasonable expectation of privacy in these records, despite the fact that they are collected and stored by a third party. *Tracey*, 152 So. 3d at 523 (citing *2011 E.D.N.Y. Opinion*, 809 F. Supp. 2d at 126). Although *Tracey* addressed real-time CSLI tracking, its Fourth Amendment analysis could be applied to historical CSLI as well—putting its decision in direct conflict with *Davis* and thus subjecting Florida residents to differing standards depending on whether a state or federal court authorizes an investigation. *See id.* (concluding same principle applies to historical and real-time CSLI).

As the dissenting judges noted in *Graham*, the majority holdings in *Graham* and *Carpenter*, "under the guise of humble service to Supreme Court precedent, markedly advance[] the frontlines of the third-party doctrine." *Graham*, 824 F.3d at 449 (en banc) (Wynn, J., dissenting). Given the broad disagreement over the proper application of the third-party doctrine, it is time for this Court to further "assess[] the application of the Fourth Amendment in the context of new technology." *Carpenter*, 819 F.3d at 897 (Stranch, J., concurring).

B. Users Do Not "Voluntarily Convey" CSLI to Providers

The judges and courts finding *Smith* does not apply to CSLI have the better argument. *Smith* rests on the holding that individuals knowingly and voluntarily convey the telephone numbers they dial to a third party. 442

U.S. at 744. But unlike when someone affirmatively dials a specific number, cell phone users do not knowingly—let alone voluntarily—transmit location data to cell providers. *See Augustine*, 4 N.E.3d at 862. It is "unlikely that cell phone customers are [even] aware that their cell phone providers collect and store historical location information." *Third Circuit Opinion*, 620 F.3d at 317. Instead, CLSI is "transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge." *S.D. Tex. 2005 Opinion*, 396 F. Supp. 2d at 756–57.

As described above, phones generate CSLI whenever they are on and searching for a signal. CSLI includes data generated when users make calls, but this data is dwarfed by the data "generated by *passive* activities such as automatic pinging, continuously running applications ("apps"), and the receipt of calls and text messages." *2015 N.D. Cal. Opinion*, 119 F. Supp. 3d at 1024 (internal quotations and citation omitted). Further, such records may be stored and turned over to the government "by any number of cellular service providers other than the cell phone user's[.]" *Id.* at 1033.

The vast majority of CSLI generated by modern cell phones is thus created "with far less intent, awareness, or affirmative conduct on the part of the user than what was at issue in . . . *Smith*." *Id.* at 1029. Such passive, unknowing generation of CSLI does not amount to a "voluntary conveyance" under the third-party doctrine. *Id.*; *see also Davis*, 785 F.3d at 534 (Martin, J., dissenting); *Tracey*, 152 So. 3d at 525–26.

Some courts have held that merely choosing to carry and turn on a phone is sufficient to meet *Smith*'s voluntary conveyance test. *See, e.g., Graham*, 824 F.3d at 428 (en banc); *Carpenter*, 819 F.3d at 888. But when a phone can be considered a "feature of human anatomy," owning and carrying a phone is hardly a choice at all. *Riley*, 134 S.Ct. at 2484; *see also City of Ontario v. Quon*, 560 U.S. 746, 760 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."). As the New Jersey Supreme Court recognized, "cell-phone users have no choice but to reveal certain information to their cellular provider," but "no one buys a cell phone to share detailed information about their whereabouts with the police." *Earls*, 214 N.J. at 584, 587.

C. The Fourth Amendment Protects Sensitive Information Even if People Know a Third Party May Access It

Smith did not create a blanket rule that all information shared with a third party is denied Fourth Amendment protection. Even if users somehow "voluntarily" convey CSLI to cell providers, this Court's decisions make clear that the fact that such highly sensitive information is held by a third party does not automatically defeat an individual's expectation of privacy. *See, e.g., Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (patient has reasonable expectation of privacy in diagnostic test results held by hospital); *Bond v. United States*, 529 U.S. 334, 338-39 (2000) (passenger retained expectation of privacy in luggage placed in bus overhead bin despite possibility of external inspection by others); *Stoner v.*

California, 376 U.S. 483, 489–90 (1963) (hotel guests entitled to constitutional protection even though they provide "implied or express permission" for third parties to access their rooms).

In *Smith* itself, the Court cautioned that a "normative inquiry" might be necessary when individuals' subjective expectation of privacy is inconsistent with "well-recognized Fourth Amendment freedoms." 442 U.S. at 740 n.5. In other words, the Fourth Amendment may still protect CSLI even if individuals voluntarily convey their location to cell providers and know that the government may seek this information from these companies.

D. Americans Reasonably Expect Location Data to Remain Private

A "normative inquiry" shows that, contrary to the conclusion reached in *Graham* and *Carpenter*, the public believes location information stored on and generated by mobile phones is private and that this expectation is reasonable. *See Oliver v. United States*, 466 U.S. 170, 178 (1984) (noting that one factor the Court uses to assess "the degree to which a search infringes upon individual privacy" is the "societal understanding that certain areas deserve the most scrupulous protection from government invasion"). When it comes to new technologies, "[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior." *Quon*, 560 U.S. at 759.

Recent studies show Americans expect privacy in their cell phones, especially when it comes to location

information. In 2014, the Pew Research Center reported that 82% of Americans consider the details of their physical location over time to be sensitive information—more sensitive than their relationship history, religious or political views, or the content of their text messages.[39] In 2012, another study found that cell phone owners take steps to protect their personal information and mobile data, and more than half of smartphone owners have uninstalled or decided to not install an app due to privacy concerns.[40] In addition, more than 30% of smartphone owners polled took affirmative steps to safeguard their privacy: 19% turned off location tracking on their phones, which disables location tracking for certain apps but does not prevent the service provider from logging CSLI.[41] The numbers are higher for teenagers, with Pew reporting 46% of teenagers turned location services off.[42] A 2013 survey conducted on behalf of Internet company TRUSTe found 69% of American smartphone users were concerned

---

39. Mary Madden, et al., *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Center 34, 36–37 (Nov. 12, 2014) *available at* http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf (50% of respondents believed location information was "very sensitive.").

40. Jan Lauren Boyles, *et al.*, *Privacy and Data Management on Mobile Devices*, Pew Research Internet & American Life Project (Sept. 5, 2012) *available at* http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/.

41. *Id.*

42. Kathryn Zickuhr, *Location-Based Services*, Pew Research Internet & American Life Project (Sept. 12, 2013) http://www.pewinternet.org/2013/09/12/location-based-services/.

about being tracked.[43] And a 2009 Carnegie Mellon survey of perceptions about location-sharing technologies showed that, on average, participants believed the risks of location-sharing technologies outweighed the benefits and were "extremely concerned" about controlling access to their location information.[44]

As noted above in Section III.A, federal and state courts have both supported the idea that it is objectively reasonable to find historical CSLI private and required the government to use a probable cause search warrant to obtain this sensitive data. Although other courts, like *Graham* and *Carpenter*, have reached the opposite conclusion, the fact that reasonable jurists have—and continue to—disagree undermines the conclusion reached in both cases that an expectation of privacy in CSLI is unreasonable.

---

43. David Deasy, *TRUSTe Study Reveals Smartphone Users More Concerned About Mobile Privacy Than Brand or Screen Size*, TRUSTe Blog (Sept. 5, 2013), http://www.truste.com/blog/2013/09/05/truste-study-reveals-smartphone-users-more-concerned-about-mobile-privacy-than-brand-or-screen-size/.

44. Janice Y. Tsai, *et al.*, *Location-Sharing Technologies: Privacy Risks and Controls*, Carnegie Mellon University 11–13 (Feb. 2010), *available at* http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

CONCLUSION

Given the prevalence of cell phones and the quantity of law enforcement requests for this sensitive information, *Graham* and *Carpenter* present questions of compelling national importance. The legal protections offered for CSLI are not uniform, and courts have issued conflicting opinions on the issue, leaving the public and law enforcement in limbo.

This Court should therefore grant *certiorari* in both *Graham* and *Carpenter* to resolve the issue, provide clear guidance to both the public and law enforcement, and ultimately conclude these sensitive records are protected by the Fourth Amendment's warrant requirement.

Dated: October 25, 2016

Respectfully submitted,

JENNIFER LYNCH
Counsel of Record
ANDREW CROCKER
JAMIE WILLIAMS
STEPHANIE LACAMBRA
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
jlynch@eff.org

RACHEL LEVINSON-WALDMAN
MICHAEL W. PRICE
BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
161 Avenue of the Americas,
12th Floor
New York, New York 10013
(646) 292-8335

Attorneys for Amici Curiae

APPENDIX

APPENDIX

The Electronic Frontier Foundation ("EFF") is a nonprofit, member-supported civil liberties organization working to protect rights in the digital world. EFF actively encourages and challenges government and the courts to support privacy and safeguard individual autonomy as emerging technologies become prevalent in society. EFF has served as *amicus* in Fourth Amendment cases before this Court, including in *City of Los Angeles v. Patel*, 135 S.Ct. 2443 (2015), *Riley v. California*, 134 S.Ct. 2473 (2014), *Maryland v. King*, 133 S.Ct. 1958 (2013), *United States v. Jones*, 132 S.Ct. 945 (2012), and *City of Ontario v. Quon*, 560 U.S. 746 (2010). EFF has also served as amicus in numerous cases addressing Fourth Amendment protections for CSLI, including, *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010); *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *Commonwealth v. Augustine*, 4 N.E.3d 846 (Mass. 2014); *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015); *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011 (N.D. Cal. 2015); and *United States v. Graham*, 824 F.3d 421 (4th Cir. 2016).

The Brennan Center for Justice at NYU School of Law is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice. The Center's Liberty and National Security ("LNS") Program uses innovative policy recommendations, litigation, and public advocacy to advance effective national security policies that respect the rule of law and constitutional values. The LNS Program is particularly concerned with domestic

intelligence gathering policies, including the dragnet collection of Americans' communications and personal data, and the concomitant effects on First and Fourth Amendment freedoms. As part of its work in this area, the Center has filed numerous *amicus* briefs on behalf of itself and others in cases involving electronic surveillance and privacy issues, including *Riley v. California*, 134 S.Ct. 2473 (2014); *United States v. Jones*, 132 S.Ct. 945 (2012); *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *petition for cert. docketed*, No. 16-402 (Sept. 28, 2016); *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016), *petition for cert. docketed*, No. 16-263 (Aug. 30, 2016); *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 829 F.3d 197 (2d Cir. 2016), *petition for reh'g* en banc *filed*, No. 14-2985 (Oct. 17, 2016); *United States v. Moalin*, No. 13-50572 (9th Cir. filed Nov. 5 1015); and *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015).

The Center for Democracy & Technology ("CDT") is a nonprofit public interest group that seeks to promote free expression, privacy, individual liberty, and technological innovation on the open, decentralized Internet. CDT supports laws, corporate policies, and technical tools that protect the civil liberties of Internet users. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

The Constitution Project ("TCP") is a constitutional watchdog that brings together legal and policy experts from across the political spectrum to promote and defend

constitutional safeguards. TCP's bipartisan Liberty and Security Committee, founded in the aftermath of September 11th, is composed of policy experts, legal scholars, and former high-ranking government officials from all three branches of government. This diverse group makes policy recommendations to protect both national security and civil liberties, for programs ranging from government surveillance to U.S. detention. Based upon their reports and recommendations, TCP files amicus briefs in litigation related to these issues. TCP is dedicated to ensuring that transformative changes in technology do not undermine the privacy rights that the Framers enshrined in our Constitution. For example, TCP's Liberty and Security Committee has published reports on public video surveillance systems (analyzing how rapid technological advances have eroded the distinction between private and public spaces in the context of such systems) and location tracking (finding that the Fourth Amendment requires law enforcement to obtain a warrant before employing GPS technology to conduct prolonged tracking of an individual's movements, even if on public streets).

The National Coalition to Protect Civil Freedoms ("NCPCF") is a coalition of 18 organizations (about half Muslim and half non-Muslim) dedicated to the preservation of our civil freedoms, particularly in the so-called War on Terror. NCPCF focuses on three areas in which civil rights have significantly eroded since 9/11: Prevention of discrimination and Islamophobia; prevention of abuse of prisoners; and prevention of preemptive prosecutions (defined as the use of pretext charges, unfair

sting operations, and generally prosecutions based on governmental suspicion of the target's ideology)

NCPCF represents the interests of Muslims and others targeted by government surveillance (which often leads to pressure to become an informant or other improper measures) based on their religion, race, country of origin, or ideology.

RECORD AND BRIEFS

FILED
AUG - 7 2017
OFFICE OF THE CLERK
SUPREME COURT, U.S.

No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

—v.—

UNITED STATES OF AMERICA,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

JOINT APPENDIX

Harold Gurewitz
Counsel of Record
GUREWITZ & RABEN, PLC
333 W. Fort Street, Suite 1400
Detroit, MI 48226
(313) 628-4733
hgurewitz@grplc.com
Counsel for Petitioner

Jeffrey B. Wall
Counsel of Record
Acting Solicitor General
UNITED STATES DEPARTMENT OF JUSTICE
950 Pennsylvania Avenue, N.W.
Washington, DC 20530-0001
(202) 514-2217
SupremeCtBriefs@USDOJ.gov
Counsel for Respondent

PETITION FOR WRIT OF CERTIORARI FILED SEPTEMBER 26, 2016

PETITION FOR WRIT OF CERTIORARI GRANTED JUNE 5, 2017

TABLE OF CONTENTS

United States District Court for the Eastern District of Michigan (Detroit), No. 2:12-cr-20218-SFC-MKM, Relevant Docket Entries 1

United States Court of Appeals for the Sixth Circuit, No. 14-1572, Relevant Docket Entries 26

United States District Court, Eastern District of Michigan, Southern Division, Case No. 12-20218

Transcript of Jury Trial - Volume Two (Dec. 6, 2013) 33

Transcript of Jury Trial - Volume Seven (Dec. 13, 2013) 35

Transcript of Jury Trial – Volume Eight (Dec. 16, 2013) 130

Defendant's Trial Exhibit No. 2, Excerpt of Records for Target Number: 313.424.957 135

Defendant's Trial Exhibit No. 3, Excerpt of Records for Target Number: 313.424.957 136

RELEVANT DOCKET ENTRIES

United States District Court for the Eastern District of Michigan (Detroit)
No. 2:12-cr-20218-SFC-MKM

United States v. Green et al.

DATE	DOCKET NUMBER	PROCEEDINGS
12/11/2012	55	FIRST SUPERSEDING INDICTMENT as to Juston Labaron Young (3) count(s) 5s, 6s, 7s, 8s, Timothy Ivory Carpenter (4) count(s) 1, 2, 3, 4. [TIME STAMPED ON 8/29/12] (KKra) (Entered: 12/12/2012)
12/14/2012		Minute Entry for proceedings held before Magistrate Judge R. Steven Whalen: Arraignment as to Timothy Ivory Carpenter (4) Count 1,2,3,4 held on 12/14/2012. Disposition: Plea of Not Guilty Entered. (Tape #: RSW 12/14/2012) (Defendant Attorney: Harold Gurewitz) (AUSA: Kenneth Chadwell) (JCur) (Entered: 12/14/2012)
02/19/2013	66	SECOND SUPERSEDING INDICTMENT as to Timothy

DATE	DOCKET NUMBER	PROCEEDINGS
		Ivory Carpenter (4) count(s) 1s, 2s, 3s, 4s, 5s, 6s, Adriane Foster (5) count(s) 5, 6, 7, 8, 9, 10. (DPer) (Entered: 02/21/2013)
04/02/2013	78	THIRD SUPERSEDING INDICTMENT as to Timothy Ivory Carpenter (4) count(s) 1ss, 2ss, 3ss, 4ss, 5ss, 6ss, 7ss, 8ss, Adriane Foster (5) count(s) 5s, 6s, 7s, 8s, 9s, 10s, Jesse Gordon Dismukes, Jr. (7) count(s) 9, 10, 11, 12, 13, 14, David Lamont Holland (8) count(s) 9, 10, 11, 12, 13, 14, Lacrystal Elice Hill (9) count(s) 13, 14. (KKra) (Entered: 04/02/2013)
07/10/2013	119	FOURTH SUPERSEDING INDICTMENT as to Timothy Ivory Carpenter (4) count(s) 1sss, 2sss, 3sss, 4sss, 7sss, 8sss, 9sss, 10sss, 11sss, 12sss, 13sss, 14sss, Sedric Charles Bell-Gill (10) count(s) 3, 4, 11, 12, Timothy Michael Sanders (11) count(s) 5, 6, 7, 8, Patrick Heard (12) count(s) 13, 14, 15, 16. (KKra) (Entered: 07/11/2013)
11/21/2013	196	MOTION in Limine *to Suppress Cell Phone Data* by Timothy

DATE	DOCKET NUMBER	PROCEEDINGS
		Michael Sanders. (Attachments: # 1 Index of Exhibits Index of Exhibits, # 2 Exhibit Exhibit A - 2703 Order) (Early, S.) (Entered: 11/21/2013)
11/22/2013	201	EXHIBIT LIST by United States of America as to Timothy Ivory Carpenter, Timothy Michael Sanders (Chadwell, Kenneth) (Entered: 11/22/2013)
11/22/2013	208	EXHIBIT LIST by Timothy Michael Sanders (Early, S.) (Entered: 11/22/2013)
11/22/2013	210	NOTICE of Joinder/Concurrence in 206 Objection filed by Timothy Michael Sanders, 208 Exhibit List filed by Timothy Michael Sanders by Timothy Ivory Carpenter as to Timothy Ivory Carpenter, Timothy Michael Sanders (Gurewitz, Harold) (Entered: 11/22/2013)
11/25/2013	211	MOTION in Limine *to Exclude Lay & Expert Testimony* by Timothy Ivory Carpenter. (Attachments: # 1 Index of Exhibits, # 2 Exhibit A: Cellular Analysis) (Gurewitz, Harold)

DATE	DOCKET NUMBER	PROCEEDINGS
		(Entered: 11/25/2013)
11/25/2013	214	NOTICE of Joinder/Concurrence in 196 MOTION in Limine *to Suppress Cell Phone Data* filed by Timothy Michael Sanders, 199 MOTION in Limine *to Exclude Certain Specified Evidence and Combined Brief* filed by Timothy Michael Sanders by Timothy Ivory Carpenter as to Timothy Ivory Carpenter, Timothy Michael Sanders (Gurewitz, Harold) (Entered: 11/25/2013)
11/26/2013	216	NOTICE *of Supplement to Notice of Joinder* by Timothy Ivory Carpenter re 214 Notice of Joinder/Concurrence, (Gurewitz, Harold) (Entered: 11/26/2013)
12/02/2013	221	RESPONSE by United States of America as to Timothy Ivory Carpenter, Timothy Michael Sanders re 211 MOTION in Limine *to Exclude Lay & Expert Testimony*, 199 MOTION in Limine *to Exclude Certain Specified Evidence and Combined Brief*, 196 MOTION in Limine *to Suppress Cell Phone Data*, 203 MOTION in Limine *Pursuant to*

DATE	DOCKET NUMBER	PROCEEDINGS
		FRE 401, 403, and 404(b) (Attachments: # 1 Index of Exhibits, # 2 Exhibit A, # 3 Exhibit B, # 4 Exhibit C, # 5 Exhibit D, # 6 Exhibit E, # 7 Exhibit F) (Chadwell, Kenneth) (Entered: 12/02/2013)
12/03/2013	223	REPLY TO RESPONSE by Timothy Ivory Carpenter as to Timothy Ivory Carpenter, Timothy Michael Sanders re 196 MOTION in Limine *to Suppress Cell Phone Data* (Gurewitz, Harold) (Entered: 12/03/2013)
12/03/2013		Minute Entry for proceedings held before District Judge Sean F. Cox: Voir Dire Begun and Concluded and Jury Impaneled on 12/3/2013 as to Timothy Ivory Carpenter (4) on Count 1sss,2sss,3sss,4sss,7sss,8sss,9sss, 10sss,11sss,12sss,13sss,14sss and Timothy Michael Sanders (11) on Count 5,6,7,8 Jury Trial set for 12/5/2013 08:30 AM before District Judge Sean F. Cox (Court Reporter: Marie Metcalf) (Defendant Attorney: Harold Gurewtiz, Jason Eggert and S. Allen Early) (AUSA: Kenneth

DATE	DOCKET NUMBER	PROCEEDINGS
		Chadwell) (JMcC) (Entered: 12/04/2013)
12/03/2013		Minute Entry for proceedings held before District Judge Sean F. Cox: Motion Hearing as to Timothy Ivory Carpenter, Timothy Michael Sanders held on 12/3/2013 re 199 MOTION in Limine *to Exclude Certain Specified Evidence and Combined Brief* filed by Timothy Michael Sanders Disposition: Resolved in Part by Parties. Stipulation to be submitted. (Court Reporter: Marie Metcalf) (Defendant Attorney: Harold Gurewitz, Jason Eggert and S. Allen Early) (AUSA: Kenneth Chadwell) (JMcC) (Entered: 12/04/2013)
12/04/2013	224	NOTICE of Joinder/Concurrence in 223 Reply to Response to Motion filed by Timothy Ivory Carpenter by Timothy Michael Sanders as to Timothy Ivory Carpenter, Timothy Michael Sanders (Attachments: # 1 Index of Exhibits Index of Exhibits, # 2 Exhibit Exhibit A - Application and Order regarding (313) 578-8507) (Early, S.) (Entered:

DATE	DOCKET NUMBER	PROCEEDINGS
		12/04/2013)
12/04/2013	225	STIPULATION by United States of America as to Timothy Ivory Carpenter, Timothy Michael Sanders. (Chadwell, Kenneth) (Entered: 12/04/2013)
12/05/2013		Minute Entry for proceedings held before District Judge Sean F. Cox: Jury Trial Begun and Continued as to Timothy Ivory Carpenter, Timothy Michael Sanders on 12/5/2013. Jury Trial set for 12/6/2013 08:30 AM before District Judge Sean F. Cox (Court Reporter: Marie Metcalf) (Defendant Attorney: Harold Gurewitz, Jason Eggert and S. Allen Early) (AUSA: Kenneth Chadwell) (JMcC) (Entered: 12/05/2013)
12/06/2013		Minute Entry for proceedings held before District Judge Sean F. Cox: Jury Trial Held and Continued as to Timothy Ivory Carpenter, Timothy Michael Sanders on 12/6/2013. Jury Trial set for 12/9/2013 08:30 AM before District Judge Sean F. Cox (Court Reporter: Marie Metcalf)

DATE	DOCKET NUMBER	PROCEEDINGS
		(Defendant Attorney: Harold Gurewitz, Jason Eggert and S. Allen Early) (AUSA: Kenneth Chadwell) (JMcC) (Entered: 12/06/2013)
12/06/2013		Minute Entry for proceedings held before District Judge Sean F. Cox: Motion Hearing as to Timothy Ivory Carpenter, Timothy Michael Sanders held on 12/6/2013 re 211 MOTION in Limine *to Exclude Lay & Expert Testimony* filed by Timothy Ivory Carpenter, 196 MOTION in Limine *to Suppress Cell Phone Data* filed by Timothy Michael Sanders Disposition: Taken Under Advisement (Court Reporter: Marie Metcalf) (Defendant Attorney: Harold Gurewitz and S. Allen Early) (AUSA: Kenneth Chadwell) (JMcC) (Entered: 12/06/2013)
12/06/2013	227	ORDER Denying Without Prejudice 211 Motion in Limine as to Timothy Ivory Carpenter (4); Denying 196 Motion in Limine as to Timothy Michael Sanders (11). Signed by District Judge Sean F. Cox. (JMcC)

DATE	DOCKET NUMBER	PROCEEDINGS
		(Entered: 12/06/2013)
12/09/2013		Minute Entry for proceedings held before District Judge Sean F. Cox: Jury Trial Held and Continued as to Timothy Ivory Carpenter, Timothy Michael Sanders on 12/9/2013. Jury Trial set for 12/10/2013 08:30 AM before District Judge Sean F. Cox (Court Reporter: Marie Metcalf) (Defendant Attorney: Harold Gurewitz, Jason Eggert and S. Allen Early) (AUSA: Kenneth Chadwell) (JMcC) (Entered: 12/09/2013)
12/10/2013		Minute Entry for proceedings held before District Judge Sean F. Cox: Jury Trial Held and Continued as to Timothy Ivory Carpenter, Timothy Michael Sanders on 12/10/2013. Jury Trial set for 12/11/2013 08:30 AM before District Judge Sean F. Cox (Court Reporter: Marie Metcalf) (Defendant Attorney: Harold Gurewitz, Jason Eggert and S. Allen Early) (AUSA: Kenneth Chadwell) (JMcC) (Entered: 12/10/2013)

DATE	DOCKET NUMBER	PROCEEDINGS
12/11/2013		Minute Entry for proceedings held before District Judge Sean F. Cox: Jury Trial Held and Continued as to Timothy Ivory Carpenter, Timothy Michael Sanders on 12/11/2013. Jury Trial set for 12/12/2013 08:30 AM before District Judge Sean F. Cox (Court Reporter: Marie Metcalf) (Defendant Attorney: Harold Gurewitz Jason Eggert and S. Allen Early) (AUSA: Kenneth Chadwell) (JMcC) (Entered: 12/11/2013)
12/12/2013		Minute Entry for proceedings held before District Judge Sean F. Cox: Jury Trial Held and Continued as to Timothy Ivory Carpenter, Timothy Michael Sanders on 12/12/2013. Jury Trial set for 12/13/2013 08:30 AM before District Judge Sean F. Cox (Court Reporter: Marie Metcalf) (Defendant Attorney: Harold Gurewitz, Jason Eggert and S. Allen Early) (AUSA: Kenneth Chadwell) (JMcC) (Entered: 12/13/2013)
12/13/2013		Minute Entry for proceedings held before District Judge Sean

DATE	DOCKET NUMBER	PROCEEDINGS
		F. Cox: Jury Trial Held and Continued as to Timothy Ivory Carpenter, Timothy Michael Sanders on 12/13/2013. Jury Trial set for 12/16/2013 09:00 AM before District Judge Sean F. Cox (Court Reporter: Marie Metcalf) (Defendant Attorney: Harold Gurewitz, Jason Eggert and S. Allen Early) (AUSA: Kennth Chadwell) (JMcC) (Entered: 12/13/2013)
12/16/2013		Minute Entry for proceedings held before District Judge Sean F. Cox: Jury Trial Held and Continued as to Timothy Ivory Carpenter, Timothy Michael Sanders on 12/16/2013. Jury Deliberation also held. Jury Trial set for 12/17/2013 09:00 AM before District Judge Sean F. Cox (Court Reporter: Marie Metcalf) (Defendant Attorney: Harold Gurewitz, Jason Eggert and S. Allen Early) (AUSA: Kennth Chadwell) (JMcC) (Entered: 12/17/2013)
12/17/2013		Minute Entry for proceedings held before District Judge Sean F. Cox: Jury Deliberations Held

DATE	DOCKET NUMBER	PROCEEDINGS
		as to Timothy Ivory Carpenter, Timothy Michael Sanders on 12/17/2013. Jury Deliberations Continued to 12/18/2013 09:00 AM before District Judge Sean F. Cox (Court Reporter: Marie Metcalf) (Defendant Attorney: Harold Gurewitz and S. Allen Early) (AUSA: Kenneth Chadwell) (JMcC) (Entered: 12/18/2013)
12/18/2013		Minute Entry for proceedings held before District Judge Sean F. Cox: Jury Trial Held and Completed as to Timothy Ivory Carpenter, Timothy Michael Sanders on 12/18/2013. Jury Deliberation also held. JURY VERDICT as to Timothy Ivory Carpenter (4) Guilty on Count 1sss,3sss,4sss,7sss,8sss,9sss,10ss s,11sss,12sss,13sss,14sss and Timothy Michael Sanders (11) Guilty on Count 5,7. Timothy Ivory Carpenter (4) Not Guilty on Count 2sss and Timothy Michael Sanders (11) Not Guilty on Count 6,8. (Court Reporter: Marie Metcalf) (Defendant Attorney: Harold Gurewitz and S. Allen Early) (AUSA: Kenneth

DATE	DOCKET NUMBER	PROCEEDINGS
		Chadwell) (JMcC) (Entered: 12/19/2013)
12/18/2013	249	Jury Verdict Form as to Timothy Ivory Carpenter (PMil) (Entered: 12/19/2013)
04/16/2014		Minute Entry for proceedings held before District Judge Sean F. Cox: Sentencing held as to Timothy Ivory Carpenter. (Court Reporter: Marie Metcalf) (Defendant Attorney: Harold Gurewitz) (AUSA: Kenneth Chadwell) (JMcC) (Entered: 04/16/2014)
04/28/2014	301	JUDGMENT as to Timothy Ivory Carpenter. Signed by District Judge Sean F. Cox. (KKra) (Entered: 04/29/2014)
04/29/2014	303	NOTICE OF APPEAL by Timothy Ivory Carpenter. Fee Status: No Fee Paid. (Gurewitz, Harold) (Entered: 04/29/2014)
09/11/2014	325	TRANSCRIPT of Jury Trial - Volume One - held on 12/05/2013 as to Timothy Ivory Carpenter, Timothy Michael Sanders. (Court Reporter/Transcriber: Marie

DATE	DOCKET NUMBER	PROCEEDINGS
		Metcalf) (Number of Pages: 152) (Appeal Purposes) The parties have 21 days to file with the court and Court Reporter/Transcriber a Redaction Request of this transcript. If no request is filed, the transcript may be made remotely electronically available to the public without redaction after 90 days. Redaction Request due 10/2/2014. Redacted Transcript Deadline set for 10/14/2014. Release of Transcript Restriction set for 12/10/2014. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date, the transcript is publicly available. (Metcalf, M) [DOCKET TEXT CORRECTED, SEE NOTICE OF CORRECTION FILED 9/12/2014] Modified on 9/12/2014 (JMcC). (Entered: 09/11/2014)
09/11/2014	326	TRANSCRIPT of Jury Trial - Volume Two - held on 12/06/2013 as to Timothy Ivory Carpenter, Timothy Michael Sanders. (Court

DATE	DOCKET NUMBER	PROCEEDINGS
		Reporter/Transcriber: Marie Metcalf) (Number of Pages: 162) (Appeal Purposes) The parties have 21 days to file with the court and Court Reporter/Transcriber a Redaction Request of this transcript. If no request is filed, the transcript may be made remotely electronically available to the public without redaction after 90 days. Redaction Request due 10/2/2014. Redacted Transcript Deadline set for 10/14/2014. Release of Transcript Restriction set for 12/10/2014. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date, the transcript is publicly available. (Metcalf, M) (Entered: 09/11/2014)
09/11/2014	327	TRANSCRIPT of Jury Trial - Volume Three - held on 12/09/2013 as to Timothy Ivory Carpenter, Timothy Michael Sanders. (Court Reporter/Transcriber: Marie Metcalf) (Number of Pages: 143)

DATE	DOCKET NUMBER	PROCEEDINGS
		(Appeal Purposes) The parties have 21 days to file with the court and Court Reporter/Transcriber a Redaction Request of this transcript. If no request is filed, the transcript may be made remotely electronically available to the public without redaction after 90 days. Redaction Request due 10/2/2014. Redacted Transcript Deadline set for 10/14/2014. Release of Transcript Restriction set for 12/10/2014. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date, the transcript is publicly available. (Metcalf, M) (Entered: 09/11/2014)
09/11/2014	328	TRANSCRIPT of Jury Trial - Volume Four - held on 12/10/2013 as to Timothy Ivory Carpenter, Timothy Michael Sanders. (Court Reporter/Transcriber: Marie Metcalf) (Number of Pages: 173) (Appeal Purposes) The parties have 21 days to file with the court and Court

DATE	DOCKET NUMBER	PROCEEDINGS
		Reporter/Transcriber a Redaction Request of this transcript. If no request is filed, the transcript may be made remotely electronically available to the public without redaction after 90 days. Redaction Request due 10/2/2014. Redacted Transcript Deadline set for 10/14/2014. Release of Transcript Restriction set for 12/10/2014. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date, the transcript is publicly available. (Metcalf, M) (Entered: 09/11/2014)
09/11/2014	329	TRANSCRIPT of Jury Trial - Volume Five - held on 12/11/2014 as to Timothy Ivory Carpenter, Timothy Michael Sanders. (Court Reporter/Transcriber: Marie Metcalf) (Number of Pages: 165) (Appeal Purposes) The parties have 21 days to file with the court and Court Reporter/Transcriber a Redaction Request of this transcript. If no request is filed, the transcript

DATE	DOCKET NUMBER	PROCEEDINGS
		may be made remotely electronically available to the public without redaction after 90 days. Redaction Request due 10/2/2014. Redacted Transcript Deadline set for 10/14/2014. Release of Transcript Restriction set for 12/10/2014. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date, the transcript is publicly available. (Metcalf, M) (Entered: 09/11/2014)
09/11/2014	330	TRANSCRIPT of Jury Trial - Volume Six - held on 12/12/2013 as to Timothy Ivory Carpenter, Timothy Michael Sanders. (Court Reporter/Transcriber: Marie Metcalf) (Number of Pages: 163) (Appeal Purposes) The parties have 21 days to file with the court and Court Reporter/Transcriber a Redaction Request of this transcript. If no request is filed, the transcript may be made remotely electronically available to the public without redaction after 90

DATE	DOCKET NUMBER	PROCEEDINGS
		days. Redaction Request due 10/2/2014. Redacted Transcript Deadline set for 10/14/2014. Release of Transcript Restriction set for 12/10/2014. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date, the transcript is publicly available. (Metcalf, M) (Entered: 09/11/2014)
09/12/2014	331	NOTICE of Correction re 325 Transcript as to Timothy Ivory Carpenter, Timothy Michael Sanders. (JMcC) (Entered: 09/12/2014)
09/12/2014	332	TRANSCRIPT of Jury Trial - Volume Seven - held on 12/13/2014 as to Timothy Ivory Carpenter, Timothy Michael Sanders. (Court Reporter/Transcriber: Marie Metcalf) (Number of Pages: 196) (Appeal Purposes) The parties have 21 days to file with the court and Court Reporter/Transcriber a Redaction Request of this transcript. If no

DATE	DOCKET NUMBER	PROCEEDINGS
		request is filed, the transcript may be made remotely electronically available to the public without redaction after 90 days. Redaction Request due 10/3/2014. Redacted Transcript Deadline set for 10/14/2014. Release of Transcript Restriction set for 12/11/2014. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date, the transcript is publicly available. (Metcalf, M) (Entered: 09/12/2014)
09/17/2014	333	TRANSCRIPT of Jury Trial - Volume Eight - held on 12/16/2013 as to Timothy Ivory Carpenter, Timothy Michael Sanders. (Court Reporter/Transcriber: Marie Metcalf) (Number of Pages: 125) (Appeal Purposes) The parties have 21 days to file with the court and Court Reporter/Transcriber a Redaction Request of this transcript. If no request is filed, the transcript may be made remotely

DATE	DOCKET NUMBER	PROCEEDINGS
		electronically available to the public without redaction after 90 days. Redaction Request due 10/8/2014. Redacted Transcript Deadline set for 10/20/2014. Release of Transcript Restriction set for 12/16/2014. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date, the transcript is publicly available. (Metcalf, M) (Entered: 09/17/2014)
09/17/2014	334	TRANSCRIPT of Jury Trial - Jury Deliberating (Questions) held on 12/17/2013 as to Timothy Ivory Carpenter, Timothy Michael Sanders. (Court Reporter/Transcriber: Marie Metcalf) (Number of Pages: 9) (Appeal Purposes) The parties have 21 days to file with the court and Court Reporter/Transcriber a Redaction Request of this transcript. If no request is filed, the transcript may be made remotely electronically available to the public without redaction after 90

DATE	DOCKET NUMBER	PROCEEDINGS
		days. Redaction Request due 10/8/2014. Redacted Transcript Deadline set for 10/20/2014. Release of Transcript Restriction set for 12/16/2014. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date, the transcript is publicly available. (Metcalf, M) (Entered: 09/17/2014)
09/18/2014	335	TRANSCRIPT of Jury Trial - Jury Questions, Testimony played for the Jury, Jury Verdicts held on 12-18-2013 as to Timothy Ivory Carpenter, Timothy Michael Sanders. (Court Reporter/Transcriber: Marie Metcalf) (Number of Pages: 38) (Appeal Purposes) The parties have 21 days to file with the court and Court Reporter/Transcriber a Redaction Request of this transcript. If no request is filed, the transcript may be made remotely electronically available to the public without redaction after 90 days. Redaction Request due

DATE	DOCKET NUMBER	PROCEEDINGS
		10/9/2014. Redacted Transcript Deadline set for 10/20/2014. Release of Transcript Restriction set for 12/17/2014. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date, the transcript is publicly available. (Metcalf, M) (Entered: 09/18/2014)
09/18/2014	336	TRANSCRIPT of Sentencing Hearing held on 04/16/2014 as to Timothy Ivory Carpenter. (Court Reporter/Transcriber: Marie Metcalf) (Number of Pages: 21) (Appeal Purposes) The parties have 21 days to file with the court and Court Reporter/Transcriber a Redaction Request of this transcript. If no request is filed, the transcript may be made remotely electronically available to the public without redaction after 90 days. Redaction Request due 10/9/2014. Redacted Transcript Deadline set for 10/20/2014. Release of Transcript Restriction set for 12/17/2014. Transcript

DATE	DOCKET NUMBER	PROCEEDINGS
		may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date, the transcript is publicly available. (Metcalf, M) (Entered: 09/18/2014)
04/13/2016	389	OPINION and JUDGMENT from U.S. Court of Appeals - Sixth Circuit as to Timothy Ivory Carpenter re 303 Notice of Appeal [Appeal Case Number 14-1572/1805] (Ahmed, N) (Entered: 04/13/2016)
07/08/2016	395	MANDATE from U.S. Court of Appeals - Sixth Circuit as to Timothy Ivory Carpenter re 303 Notice of Appeal filed by Timothy Ivory Carpenter [Appeal Case Number 14-1572/14-1805] (SSch) (Entered: 07/19/2016)
09/30/2016	410	LETTER from the US Supreme Court that a petition for writ of certiorari was filed on 09/26/2016 as to Timothy Ivory Carpenter [Supreme Court Case Number: 16-402] [Court of Appeals Case Number: 14-1572] (Ahmed, N)

DATE	DOCKET NUMBER	PROCEEDINGS
		(Entered: 09/30/2016)
06/06/2017	431	LETTER from the US Supreme Court granting the petition for writ of certiorari as to Timothy Ivory Carpenter [Supreme Court Case Number: 16-402] [Court of Appeals Case Number: 14-1572] (Ahmed, N) Modified on 6/12/2017 (DPer). (Entered: 06/12/2017)
07/10/2017	439	LETTER from the US Supreme Court granting the petition for writ of certiorari as to Timothy Ivory Carpenter [Supreme Court Case Number: 16-402] [Court of Appeals Case Number: 14-1572] (Ahmed, N) (Entered: 07/10/2017)

RELEVANT DOCKET ENTRIES

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT
NO. 14-1572

United States v. Carpenter

DATE	DOCKET NUMBER	PROCEEDINGS
05/07/2014	1	Criminal Case Docketed. Notice filed by Appellant Timothy Ivory Carpenter. Transcript needed: y. (RB)
03/02/2015	25	APPELLANT BRIEF filed by Mr. Harold Z. Gurewitz for Timothy Ivory Carpenter. Certificate of Service:03/02/2015. Argument Request: requested. (HZG)
03/02/2015	26	APPENDIX filed by Mr. Harold Z. Gurewitz for Timothy Ivory Carpenter. Volume: 1; Pages: App 001 - App 019. Certificate of Service: 03/02/2015. (HZG)
03/09/2015	29	AMICUS BRIEF filed by *Nathan Freed Wessler for American Civil Liberties Union, American Civil Liberties Union of Michigan, Brennan Center for Justice,*

DATE	DOCKET NUMBER	PROCEEDINGS
		Center for Democracy & Technology, Electronic Frontier Foundation, National Association of Criminal Defense Lawyers. Certificate of Service:03/09/2015. [14-1572, 14-1805] (NFW)
03/10/2015	33	APPENDIX filed by Mr. Nathan Freed Wessler for American Civil Liberties Union of Michigan, Brennan Center for Justice, EFF, NACDL, ACLU and Center for Democracy & Technology in 14-1572, 14-1805. Volume: I-XXIX; Pages: 1 - 667. Certificate of Service: 03/10/2015. [14-1572, 14-1805] (NFW)
03/10/2015	34	MOTION filed by Mr. Nathan Freed Wessler for American Civil Liberties Union of Michigan, Brennan Center for Justice, EFF, NACDL, ACLU and Center for Democracy & Technology in 14-1572, 14-1805 to take judicial notice. Certificate of Service: 03/10/2015. [14-1572, 14-1805] (NFW)
03/20/2015	37	RESPONSE in opposition filed regarding a motion to take judicial notice, [34]; previously

DATE	DOCKET NUMBER	PROCEEDINGS
		filed by Mr. Nathan Freed Wessler in 14-1572, 14-1805. Response from Attorney Mr. Kenneth Ray Chadwell, Jr. for Appellee USA in 14-1572, 14-1805 Certificate of Service:03/20/2015. [14-1572, 14-1805] (KRC)
05/06/2015	41	APPELLEE BRIEF filed by Mr. Evan Howard Caminker for USA in 14-1572, 14-1805. Certificate of Service:05/06/2015. Argument Request: requested. [14-1572, 14-1805] (EHC)
05/26/2015	44	REPLY BRIEF filed by Attorney Mr. Harold Z. Gurewitz for Appellant Timothy Ivory Carpenter. Certificate of Service:05/26/2015. (HZG)
08/10/2015	46	ADDITIONAL CITATION filed by Mr. Harold Z. Gurewitz for Timothy Ivory Carpenter and Mr. S. Allen Early for Timothy Michael Sander. Certificate of Service: 08/10/2015. [14-1572, 14-1805]--[Edited 08/11/2015 by RB] (HZG)
08/13/2015	48	Oral argument date set for 9:00

DATE	DOCKET NUMBER	PROCEEDINGS
		a.m. on Wednesday, October 14, 2015. Notice of argument sent to counsel on 08/13/2015. [14-1572, 14-1805] (LAG)
08/18/2015	51	RESPONSE in opposition filed regarding an additional citation, [46]. Response from Attorney Mr. Evan Howard Caminker for Appellee USA in 14-1572, 14-1805. Certificate of Service:08/18/2015. [14-1572, 14-1805] (EHC)
09/09/2015	53	Amicus MOTION filed by Mr. Nathan Freed Wessler for American Civil Liberties Union of Michigan, Brennan Center for Justice, EFF, NACDL, ACLU and Center for Democracy & Technology in 14-1572, 14-1805 requesting leave to appear at oral argument. Certificate of Service: 09/09/2015. [14-1572, 14-1805] (NFW)
09/15/2015	54	ORDER filed the motion filed by Mr. Nathan Freed Wessler for American Civil Liberties Union, American Civil Liberties Union of Michigan, Brennan Center for Justice, EFF, NACDL and Center

DATE	DOCKET NUMBER	PROCEEDINGS
		for Democracy & Technology to participate in oral argument is GRANTED. Oral argument will be extended by five minutes per side. Entered by order of the court. [14-1572, 14-1805] (RB)
10/14/2015	59	CAUSE ARGUED by Mr. Nathan Freed Wessler for Amici Curiae American Civil Liberties Union of Michigan, Brennan Center for Justice, EFF, NACDL, ACLU and Center for Democracy & Technology, Mr. Harold Z. Gurewitz for Appellant Timothy Ivory Carpenter and Mr. Evan Howard Caminker for Appellee USA before Guy, Circuit Judge; Kethledge, Circuit Judge and Stranch, Circuit Judge. (MCP)
11/02/2015	58	ADDITIONAL CITATION filed by Mr. Evan Howard Caminker for USA in 14-1572, 14-1805. Certificate of Service: 11/02/2015. [14-1572, 14-1805] (EHC)
04/11/2016	60	ORDER filed we decline to take notice of Exhibits A, B, D and E. We need not take judicial notice of Exhibits C and F, which are already part of the record under

DATE	DOCKET NUMBER	PROCEEDINGS
		consideration on appeal. Ralph B. Guy, Jr., Circuit Judge; Raymond M. Kethledge, Circuit Judge and Jane Branstetter Stranch, Circuit Judge. [14-1572, 14-1805] (RB)
04/13/2016	61	OPINION and JUDGMENT filed : The judgments in both cases are AFFIRMED. decision for publication. Ralph B. Guy, Jr., Raymond M. Kethledge (AUTHORING), and Jane Branstetter Stranch (CONCURRING), Circuit Judges. [14-1572, 14-1805] (CL)
05/26/2016	64	PETITION for en banc rehearing filed by Mr. Harold Z. Gurewitz for Timothy Ivory Carpenter. Certificate of Service: 05/26/2016. (HZG)
06/29/2016	65	ORDER filed denying petition for en banc rehearing [64] filed by Mr. Harold Z. Gurewitz. Ralph B. Guy , Jr., Raymond M. Kethledge, and Jane Branstetter Stranch, Circuit Judges. (BLH)
07/08/2016	66	MANDATE ISSUED with no costs taxed. [14-1572, 14-1805]

DATE	DOCKET NUMBER	PROCEEDINGS
		(RB)
09/30/2016	67	U.S. Supreme Court notice filed regarding a petition for a writ of certiorari filed by Appellant Timothy Ivory Carpenter. Supreme Court Case No:16-402, 09/26/2016. (CL)
06/06/2017	68	U.S. Supreme Court letter filed GRANTING the petition for a writ of certiorari [67] filed by Timothy Ivory Carpenter. Supreme Court Case No: 16-402, 06/05/2017. **N.B. ERRATUM - THE PETITION FOR WRIT OF CERTIORARI WAS GRANTED.- -[Edited 07/10/2017 by CL] (CL)

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

-v-

Case No.
12-20218

TIMOTHY IVORY CARPENTER and
TIMOTHY MICHAEL SANDERS,

Defendants.

JURY TRIAL - VOLUME TWO
BEFORE HON. SEAN F. COX
United States District Judge
257 U.S. Courthouse
231 West Lafayette Boulevard
Detroit, Michigan 48226

(Friday, December 6, 2013)

APPEARANCES:

KENNETH R. CHADWELL, ESQUIRE
Appearing on behalf of the
Government.

HAROLD Z. GUREWITZ, ESQUIRE
JASON EGGERT, ESQUIRE
Appearing on behalf of the
Defendant Timothy Ivory
Carpenter.

S. ALLEN EARLY, ESQUIRE
Appearing on behalf of Defendant
Timothy Michael Sanders.

DATE	DOCKET NUMBER	PROCEEDINGS
		(RB)
09/30/2016	67	U.S. Supreme Court notice filed regarding a petition for a writ of certiorari filed by Appellant Timothy Ivory Carpenter. Supreme Court Case No:16-402, 09/26/2016. (CL)
06/06/2017	68	U.S. Supreme Court letter filed GRANTING the petition for a writ of certiorari [67] filed by Timothy Ivory Carpenter. Supreme Court Case No: 16-402, 06/05/2017. **N.B. ERRATUM - THE PETITION FOR WRIT OF CERTIORARI WAS GRANTED.- -[Edited 07/10/2017 by CL] (CL)

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

-v-

Case No.
12-20218

TIMOTHY IVORY CARPENTER and
TIMOTHY MICHAEL SANDERS,

Defendants.

JURY TRIAL - VOLUME TWO
BEFORE HON. SEAN F. COX
United States District Judge
257 U.S. Courthouse
231 West Lafayette Boulevard
Detroit, Michigan 48226

(Friday, December 6, 2013)

APPEARANCES:

KENNETH R. CHADWELL, ESQUIRE
Appearing on behalf of the
Government.

HAROLD Z. GUREWITZ, ESQUIRE
JASON EGGERT, ESQUIRE
Appearing on behalf of the
Defendant Timothy Ivory
Carpenter.

S. ALLEN EARLY, ESQUIRE
Appearing on behalf of Defendant
Timothy Michael Sanders.

* * * * *

[158]

Mr. Gurewitz's motion with respect to *Daubert* and I join in his comments now, Your Honor.

THE COURT: Okay. Anything else, Mr. Chadwell?

MR. CHADWELL: I guess I'm just inclined now to reply to Mr. Gurewitz's reply --

THE COURT: Sure. Go ahead.

MR. CHADWELL: As I understand Mr. Gurewitz's reply brief, he was highlighting -- he seemed to be abandoning his other arguments and he was highlighting that he didn't think the reasonable ground standard had been met.

THE COURT: Right.

MR. CHADWELL: And so I just wanted to say a few words about the 2703(d) reasonable ground standard, if I could. And if you read 2703(d) carefully, there's a lot of qualifiers if you look carefully. First of all, reasonable grounds is less than probable cause. That's kind of a big qualification.

Then reasonable grounds to believe that something is relevant, which is a another gigantic qualification, what might be relevant to something can be really far afield. It's giant umbrella of information. And thirdly, we don't have to show a crime. We merely have to show there's a criminal investigation of a crime, which is a third qualifier. And then, even when we don't meet the statute full

* * * * *

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

-v-

Case No.
12-20218

TIMOTHY IVORY CARPENTER and
TIMOTHY MICHAEL SANDERS,

Defendants.

JURY TRIAL - VOLUME SEVEN
BEFORE HON. SEAN F. COX
United States District Judge
257 U.S. Courthouse
231 West Lafayette Boulevard
Detroit, Michigan 48226

(Friday, December 13, 2013)

APPEARANCES:

KENNETH R. CHADWELL, ESQUIRE
Appearing on behalf of the
Government.

HAROLD Z. GUREWITZ, ESQUIRE
JASON EGGERT, ESQUIRE
Appearing on behalf of the
Defendant Timothy Ivory
Carpenter.

S. ALLEN EARLY, ESQUIRE
Appearing on behalf of Defendant
Timothy Michael Sanders.

* * * * *

[32]

prevention training in a store after the fact. A loss prevention manager would, to kind of reinforce security measures, what should be done, what shouldn't be done, this type of situation.

Q Where is the loss prevention manager for Warren, Ohio?

A He would be based out of Cleveland right now, I believe.

Q Cleveland?

A Yes.

Q Was that the case back in 2011?

A At the time, I believe it was Pittsburgh.

MR. EARLY: Pittsburgh. Thank you.

THE COURT: Redirect?

MR. CHADWELL: No questions, Your Honor.

THE COURT: Thank you very much, Mr. Decker.

THE WITNESS: Thank you.

MR. CHADWELL: Your Honor, I call Chris Hess at this time.

THE COURT: Would you give your full name to our court reporter, please?

THE WITNESS: Christopher Hess.

SPECIAL AGENT CHRISTOPHER HESS, GOVERNMENT'S WITNESS, SWORN DIRECT EXAMINATION

BY MR. CHADWELL:

Q Please repeat your name?

A Christopher Hess.

[33]

Q How are you employed?

A I'm a Special Agent with the Federal Bureau of Investigation.

Q How long have you been with the FBI?

A Just over nine and-a-half years.

Q What's your formal educational background?

A I have an undergraduate degree in business administration and a master's degree in public administration.

Q And have you worked as a police officer anyplace else?

A I have.

Q Where?

A In the City of White Plains in New York, and the town of Mount Pleasant in New York.

Q And what have you done within the FBI?

A I'm assigned to the Detroit division and I'm assigned to the violent crime task force.

In addition to my daily assignment to the task force, I'm on the SWAT team and a member of the cellular analysis survey team.

Q What does the violent crime task force do?

A The violent crime task force is a joint task force between federal agencies, state and local

agencies, and we investigate a variety of violent criminal acts, including kidnappings, gang activity, robbery, homicide, fugitives, kidnappings, extortion.

[34]

Q And do you use your cellular analysis involvement to assist your work with the violent crimes task force?

A Yes, I do.

Q Do you also assist state and local officials in some of their cases?

A Yes.

Q What kinds of things would you assist state and local people with in reference to cellular analysis?

A I've provided assistance in a variety of cases, from public corruption to violent incident crimes to serial homicide investigations, as well as national security investigations and white-collar types of investigations.

Q Could you tell the jury about what the CAST team is?

A CAST is the acronym we use for the Cellular Analysis Survey Team. It's a group of agents within the FBI who have received specialized training with regard to how cell phones and cell phone companies produce their records, how the cell phones operate, how their networks operate.

At this point in time there is roughly 30 agents in the FBI who have gone through the

certification process. I was one of the first ten to do it.

Q Are you now also involved in teaching other FBI agents?

A Yes, and other law enforcement as part of our responsibility.

Q What kind of teaching have you had in that regard?

[35]

A Well, I've conducted courses for state and local, as well as other federal agents and law enforcement entities, including prosecutors, with regard to the use of cell phone technology investigations.

Q Have you spoken at conferences, FBI Academy, Department of Justice?

A Yes, I've presented at different conferences. Yes.

Q How much training did you go through to be certified by the FBI in cellular analysis?

A It's well over 400 hours of training that I have personally participated in.

Q And who conducts the training of the FBI?

A There is a variety of entities, private corporations. The bulk of our training comes directly from the cellular providers, including their law enforcement relations which handles the legal requests for the records, as well as the engineers from the various companies to explain how their individual companies operate.

Q Okay. And these are the companies that actually construct and place cell towers?

A Yes.

Q Throughout the United States?

A Yes.

Q They monitor their own cell towers?

A Yes, they do.

[36]

Q They have engineers to determine if, say, another cell tower is needed in a particular area or not?

A Yes.

Q And what are these companies?

A The major providers that we might have received training from would be Verizon, Sprint-Nextel, Metro PCS, US Cellular, T-Mobile, AT&T, Cricket.

Q And how many agents would you say that have now been involved in training?

A The last count, somewhere between 1500 and 2,000.

Q Okay. And I assume they're not all located in Michigan, this is throughout the United States?

A Correct.

Q So you've been recognized by other agencies other than the FBI as having expertise in this area?

A Yes.

Q And other law enforcement agents who have received your training then go on to work cases?

A Yes, they do.

Q And what kind of cases would cellular analysis be useful in and how would these investigators use that?

A Well, I would say that cell phone analysis is pretty applicable to just about any investigation out there, again, from terrorist investigations right down to a simple larceny investigation.

[37]

Q Let me ask you about a recent case you were involved in.

There was a murder out in Ann Arbor and some suspects were tracked down in another state.

A That's presently in litigation, so --

Q So we don't want to discuss cases that are in litigation.

A Correct.

Q But have you been involved in cases where people had to be tracked down through cellular technology?

A Yes.

Q Okay. And you've successfully been able to track people?

A Yes.

Q Locate people who are wanted for whatever?

A Yes.

Q How many cases have you personally worked on involving cellular record analysis?

A Well over 100, I would say.

Q And can you just go through some of the cases, not in litigation, but the types of cases?

A Personally, I've used the analysis in my own investigations with regard to gang activity. I have used it successfully in some serial homicide investigations, kidnappings, Amber alerts where successfully located a child that was the victim of a kidnapping, as well as the perpetrators who conducted the kidnapping.

Phone robbery investigations, I've used it both [38] where I was the case agent, as well as providing assistance to other investigators.

I've used it in white-collar and corruption cases where there was organized crime.

Bribing city council members in another jurisdiction, we were able to use cell phone analysis to corroborate information.

Q And so being trained in cellular analysis is one thing theoretically, but you actually put it into play in 100 cases or more?

A Absolutely, yes.

Q Okay. And so you've seen how it works out, right? You can theoretically be taught things by these cellular carriers, but having been taught them, you've applied them to cases?

A Yes. Practical experience, yes.

Q And what you've been taught has proven out to be accurate in these cases; --

A It has been reliable, yes.

Q -- is that right?

So what you thought was true, hypothetically, you have proven to be true through your experience?

A Yes.

Q And you testified previously in federal court as an expert witness in this area?

[39]

A I have.

Q In what courts and approximately how many times?

A Approximately, in the ballpark of 30 or more times. And I've testified here in the Eastern District of Michigan, the Western District of Michigan, the District of Rhode Island, Virginia, for federal court and state court. I've testified here in Michigan on a number of occasions.

Q Sir, directing your attention to this case, were you asked to perform a cellular telephone record analysis?

A I was.

Q And can you tell the jury, in general, how does a cellular telephone work?

A A cellular telephone is a two-way radio in the simplest of terms. It transmits a frequency and it receives a frequency. And those frequencies are tuned with your cell phone carrier. So if you

have a Verizon phone, you tune into Verizon towers to communicate, to have your telephone calls go back and forth.

Q So the towers communicate with the phone and the phone's communicating with the tower?

A Correct.

Q And are there occasions where someone who might have a Verizon phone might end up on another carrier's tower?

A In a roaming situation, if Verizon doesn't have coverage in a particular area of the country, they would have an [40] agreement with another company to be able to utilize their infrastructure.

Q And what determines what tower the cell phone is going to be communicating with?

A When your cell phone is in an idle mode, it's constantly scanning the environment for radio frequencies, and it's looking for a strong signal from the provider that your telephone is with. And as it moves around, that information is constantly calculated and it changes. So if I'm in the influence of this tower at one moment and I start to move around, the towers that I'm starting to get closer to, their signal strength improves and the phone chooses that as its serving cell site.

Q So the phone is constantly looking for a friend to communicate with?

A Yes, yes.

Q And it likes the strongest one, in general?

A Yes.

Q What would the tower with the strongest signal be referred to by someone like you?

A As a serving cell.

Q Okay. Can you describe for the jury how a cell tower works as distinguished from the phone?

A Again, a cell tower is a large antenna that emits a radio frequency and it puts out identifying information for its [41] subscribers to let them know that you are in the area of your carrier. "Here's a Metro PCS cell phone tower. Use me when you're in this area."

Q Okay. And are cell towers different from one another?

A In what regard?

Q They come in different shapes and sizes or --

A Yes.

Q Do they have particular sides or --

A Cell towers are broken down into what they call sectors. In most cases, a cell site will cover 360 degrees. And often the tower is broken down into three sectors which allows for an increase in usage on the tower. So that if somebody was on the north side of the tower, they use the north side of the tower, the north sector.

If they're on the south side of the tower, they use the south side.

Q So each sector would be 120 degrees each --

A Roughly, yes.

Q -- to cover the 360?

And does each of these three sectors send a different signal, like in a certain direction?

A Yes. There is differentiation in the signal.

Q Okay. So if a cell phone -- if a guy is driving with a cell phone down I-75 and there's a cell tower, is it possible that the phone will be communicating with this particular [42] tower in one sector when they're on one stretch of 75 and then as they head down the road, switch to a different sector?

A Yes.

Q Of that tower?

A Yes.

Q And if maybe they got off 75 and took a right-hand turn, they might even, depending on the angle, start communicating with the third sector of the same tower?

A Correct.

Q If that turned out to be the closest tower, right?

A Yes.

Q And how and why are towers positioned in certain locations?

A The number of towers in an area is largely dependent upon the number of subscribers in the area. So when you have an urban environment where there are a lot more people, a lot more population, cell companies will put more towers, more antennas in the area to handle that volume.

When you're out in a rural area, perhaps not as many towers, and also taking into consideration things like topography and construction in the area.

So in Chicago, let's say, there's a lot of high-rises. There may be a larger number of towers to cover areas that would be obstructed by the buildings.

[43]

And if you have a mountain range, they would change the orientation of the towers.

Q And do towers overlap one another in coverage?

A Yes. There is a degree of overlap, sort of the, "Can you hear me now" commercials from Verizon.

Q So there could be Verizon towers that have kind of overlapping coverage of each other?

A Yes. There's boundaries to the towers but they want to -- the companies want to make sure that they fill as much of the space as they possibly can so they don't drop your calls.

Q Okay. And how far away can a tower send a signal and/or a cellular telephone receive a signal?

A Theoretically, if a tower is at full power and there's no angle and there is no interference, a tower can go up to 20 miles. But the limiting factor, and it is the power of the cell phone, which would not be able to communicate back to the cell phone tower.

So in an area like Detroit, in my experience, typically you would see coverage for a particular cell site anywhere from a-half mile to two miles.

Q And are antennas of cell towers pointed upside down?

A The antennas are at the top of poles or at the top of a building, and in that, completely perpendicular to the ground. They are actually angled down towards the ground to direct the radio frequency to a particular area.

[44]

Q I think you said some of this already, but what are all the factors that affect the propagation of a signal from a tower?

A Oh, certainly buildings, topography, so the shape of the earth, the -- again, if there are mountains or hills. The time of year has an effect on it to some degree, whether there are leaves on the trees or no leaves on the trees. Weather to some degree may have an effect on the signal.

Q Now, can you determine by any degree of certainty the area that each sector of a cell tower is covering?

A Yes. Based on training and experience, we can come up with a geographic area for that coverage.

Q What's a tower's footprint?

A The footprint would be what the coverage area is of a particular sector or the entire coverage area of the cell site.

Q Now, the signals kind of put out away from the tower; is that what the tower is doing?

A Yes.

Q And how is that signal able to be measured or observed?

A Well, there is the chips or the computers inside the phones are measuring what the signal strength is received off of that tower.

Q And how do cellular providers measure the signals that their towers are producing and try to determine if they need [15] more towers, what kinds of instrumentation do they use?

A Well, the engineers would use equipment that measures signal strength, and do various testing, drive testing and also monitor from -- they have like emergency operations centers or operation centers that monitor the activity and the performance of the networks.

Q I think you have already said that some of the big companies have their own cell towers and sometimes they share towers?

A Yes. In most cases the large companies have their own cell sites. The smaller mom and pop type of companies would use those large companies' towers.

Q Okay. And can different companies share even the same pole?

A Yes. I'm sure most have seen a cell site where there's numerous antennas at the top, and those would represent different companies. So somebody may own the physical pole itself and

then lease space to each of the different providers.

Q Now, as the companies are maintaining these towers and selling cell service to people, making money with these things and determining how many towers they need where in the best possible way, what kind of records do they keep of their cellular activity to assist them in their business?

A They would use -- they would keep call detail records for [46] the telephone usage by their provider -- excuse me, by their subscribers.

Q What's included in call detail records?

A Call detail records would contain the date and time of a call, the length of the call, what numbers were engaged in that call, who called you or who did you call, any special features like call waiting or call forwarding, as well as the cell sites. And in most instances now, the companies provide you -- provide information on the tower where the call originated and the tower where the call terminated.

Q And do they collect and store data related to the cell towers themselves, also?

A Yes.

Q Sir, how did you come to be involved in this case? This is not to case, right?

A No, I am not the case agent on this.

Q How did you get involved in this case?

A I was asked to provide assistance by Agent Ruiz.

Q And what assistance did you provide?

A He asked that I review two telephone numbers to try and determine if, in fact, they were in the area of a series of robberies, in and around the time of the robbery.

Q And did you review call detail records from T-Mobile, Metro PCS and Sprint?

A I did.

[47]

MR. CHADWELL: Your Honor, at this time I would offer into evidence a stipulation of the parties, Government Exhibit 58.

THE COURT: Sure.

MR. CHADWELL: I would like to read the stipulation at this time.

MR. EARLY: No objection.

MR. GUREWITZ: No objection.

THE COURT: Go ahead.

MR. CHADWELL: Okay.

"The parties stipulate and agree that the telephone call detail records from T-Mobile, Metro PCS and Sprint utilized by FBI Special Agent Christopher Hess to formulate his analysis and opinion are authentic and accurate business records of these companies."

THE COURT: All right. The stipulation is received.

MR. CHADWELL: Thank you, Your Honor. If I can just have a moment, Your Honor?

BY MR. CHADWELL:

Q Now, sir, I'm showing you what's been marked as Government Proposed Exhibit 57.

Do you recognize that document?

A I do.

Q What is that document?

[18]

A It's a report that I prepared with regard to the cell phone analysis I conducted.

Q So you reviewed the records we have been discussing here from the three companies, the call detail records?

A Yes.

Q In reference to two different telephone numbers?

A Yes.

Q And you reduced your analysis to a written form; is that right?

A Yes.

Q You prepared charting as part of this also?

A Correct.

Q And that's the document in front of you?

MR. CHADWELL: Your Honor, I move the admission of Government 57 at this time.

THE COURT: Any objection?

MR. GUREWITZ: Could I just confer with Mr. Chadwell about this?

(Discussion off record)

MR. GUREWITZ: I have no objection.

THE COURT: Mr. Early?

MR. EARLY: None, Your Honor.

THE COURT: All right. Exhibit 57 is received.

MR. CHADWELL: Thank you, Your Honor.

BY MR. CHADWELL:

[49]

Q And as we go through this, hopefully that's a good enough copy in front of you to refer to. We also will be using the big-screen also.

Sir, as part of your analysis, let's talk about the first phone number that you analyzed in reference to call detail records of these mobile telephone companies that we have been talking about.

What is the first telephone number that you --

A The first number is (313) 579-8507.

Q And, sir, is that the same number that appears on this board back here next to the name Big Tim?

A Yes.

Q Sir, what did you determine from your review of call detail records in reference to that telephone number pertaining to the date of March 4, 2011?

A That was a T-Mobile telephone number and there was a reported robbery March 4, 2011 at 2:52 p.m. in Warren, Ohio at a RadioShack.

And review of the call detail records and tower records in and around that time, that cell phone

used a cell site within proximity to the RadioShack in Warren.

Q Did you prepare a map to kind of illustrate that?

A I did.

Q Okay. And that's part of this in front of you? It's a little bit off screen.

[50]

Sir, what area is this a map of?

A This is a map of Warren, Ohio.

Q And there is a blue square as part of this map; is that right?

A Yes.

Q What is that location?

A That represents the RadioShack at 2553 Parkman Road N.W. in Warren, Ohio.

Q That's right here (indicating)?

A Yes, sir.

Q And then there's a red dot. What does that represent?

A That depicts the T-Mobile cell site.

Q And there is two calls that are highlighted at the top of your chart here. What does that represent?

A The nearest call to the reported time of the robbery was at 2:20 p.m. on that date, and that number -- or that call is highlighted, that's line 7738, the yellow highlighted area.

Q It says that call lasted 31 minutes?

A Yes.

Q And then there was a second call too, that you looked at?

A Yes. The next call after that was at 3:12 p.m., less than a minute, utilizing the same cell site.

Q Okay. And were you able to determine the location of the phone with the number 579-8507?

A Based on the columns of -- column D and E, combined with [51] the columns H and I, you have the first LAC, which is the location area code, which would be -- the analogy would be to a ZIP Code.

And then the number that's associated with first cell, last cell, would be similar to like your street address. So in other words you could have 123 Main Street in 100 cities across the country, but based on ZIP Code, we would know that it's in Warren, Ohio. The 8499 is the ZIP Code and I know that that cell site is in Warren, Ohio.

Q Okay. So the 8499 I'm reading up there is the code?

A Yes.

Q That's used by the cellular telephone companies?

A Correct.

Q That indicate particular tower and location?

A That would indicate a geographic region of the country.

Q Okay. And I see that you have drawn lines out from the red dot tower; is that right?

A Yeah, right.

Q Does that represent a sector?

A That illustrates the sector, yes.

Q So there's two other sectors. If we drew out the lines we would see two other sectors; is that right?

A Yes.

Q But on the date and time of the robbery, that cellular telephone was in that -- in the sector closest to the [52] RadioShack?

A Yes.

Q Is that your conclusion?

A Yes.

Q Sir, I want to also ask you if you looked at or analyzed call detail records including tower locations for a second telephone number?

A I did.

Q What was that second telephone number?

A (313) 412-6845.

Q And, sir, is that the same number that we see on the board next to the name Little Tim?

A Yes, on the bottom of the board.

Q Little is misspelled as "Lil" at the bottom?

A Yes.

Q 412-6845?

A Yes.

Q Sir, did you look at several dates pertaining to that number?

A I did.

Q Let's start with the first date that you looked at and location.

A The first date was December 13, 2010. I reported a time of 10:35 a.m.

Q Okay. And you created a map and a chart?

[53]

A Yes.

Q To illustrate your conclusions from that?

A Yes.

Q And again, we have a blue square on your chart right here (indicating)?

A Yes.

Q What is that blue square?

A That represents the location of a RadioShack at 13330 Jefferson Avenue in Detroit.

Q Okay. And we also have some various red dots throughout this. What are those?

A The red dots represent the Metro PCS towers in that area.

Q That was a Metro PCS phone?

A Correct.

Q And there's a dot here with a sector drawn out?

A Yes.

Q And so what does this tell us in terms of your conclusions as to the location of the telephone, 412-6845, on December 13, 2010 at around the time of the robbery?

A Well, based on the two calls that are highlighted, the telephone used cell sites on the east side and particularly used cell sites with sectors that would be consistent with the geographic area that encompasses the robbery scene.

Q And so can you tell us approximately when that phone was where?

[54]

A Well, at 10:24 a.m. there was a telephone call that originated and terminated on tower 127, which is the dot just to the southwest of the robbery scene. And it used two sectors on that tower for the originating and terminating.

And then at 10:31 a.m., there was a call that was eight minutes in duration that was on tower 145, which is just to the northeast of the robbery location, utilizing a sector oriented towards or in the direction of where the robbery location is depicted, and then that call terminated on a tower at the top of the map along I-94.

Q Okay. So just to be clear, this first call up here, 10:24?

A Yes.

Q The phone is down near this tower (indicating)?

A Yes.

Q In one or both of these sectors (indicating)?

A It starts in one and ends in another.

Q So we can see two sectors off this tower, right?

A Right.

Q So at 10:24 the phone is in one of these two sectors going back and forth, right?

A Yes.

Q Later on the same day, seven minutes later, there is a call and now the phone is within this sector up here, (indicating) right? It's no longer hitting off this tower.

[55]

It is traveling in this direction (indicating)?

A Right. It's on a different tower, a different sector.

Q Okay. The direction it traveled is -- from this tower, the direction traveled was towards the RadioShack; is that right?

A Yes.

Q And after traveling towards the RadioShack at this time while this call is still going on, it later ends up in this direction (indicating)?

A Yes.

Q And it starts bouncing off that tower on the top?

A Well, the call that originated on the -- the call that originated on tower 145 ended on tower 164, which is the one that's up towards the freeway there.

Q And which one is 145 again?

A One-forty-five is the one just to the northeast of the robbery location.

Q The northeast being this way (indicating) on the map?

A Yes, towards the upper right-hand corner.

Q Sir, did you also perform an analysis of this same telephone number for December 18, 2010?

A Yes.

Q And for what location?

A This was related to a T-Mobile robbery or the robbery of a T-Mobile store. On the police report, I believe it was [56] 4:50 p.m., and that robbery location was 14304 Gratiot Avenue, in Detroit.

Q And again we have a blue square, kind of in the upper middle of that chart; is that right?

A Yes.

Q What does that represent?

A That's the location of the T-Mobile store at 14304 Gratiot.

Q And you have some phone calls that you used to do this tracking. And I'm not sure if we made it clear when I originally asked you some preliminary questions, but you are not able to do this unless the phone is active; is that correct?

A Correct.

Q And what's it take for the phone to be active?

A Engaging in a call, receiving or sending a call.

Q So if the phone is just in my pocket, and I'm not calling and no one is calling me, you couldn't really do this?

A Right. It's not populated in the call detail records.

Q Even though it might be communicating in there, --

A That's correct.

Q -- searching for a tower or whatever, but it's the actual call itself that enables you to get a strong enough signal to do what we're talking about here?

A Yes. So when the phone requests resources, in other [57] words, for example, if you dial a number and you hit send, that tower information is populated in the call detail record.

Q Okay. So, sir, based on these calls, what can you tell us about the location of the 412-6845 phone at around the time of the robbery and at around the location of the robbery?

A There was a call at 4:46. It was an outgoing call that started on tower 173, which is down the center of the map, the lower dot.

Q Right down here (indicating)?

A Yes.

Q Okay. And you have an arrow pointing to the right. Is that meant to be part of a sector?

A It represents the orientation of the cell sector, what direction that signal is emanating.

Q So the phone starts out here, right?

A Yes.

Q At 4:46?

A Correct.

Q And where does the phone go from there?

A Then it terminates on a cell site just to the north, which is cell site 188, sector four.

Q Okay. Is that this cell site here (indicating)?

A Correct.

[58]

Q So the phone has gone from here to here (indicating); is that right?

A Yes.

Q Which is in the general direction of the T-Mobile we have been talking about?

A Yes.

Q And did that cover both calls up there?

A The next call at 4:53 originated and terminated on tower 188, sector one, which was granted to the 12 o'clock direction.

Q So this is 188 again?

A Yes.

Q You say it's oriented toward 12 o'clock, meaning this way (indicating)?

A Yes, to the north.

Q So the phone, according to the records you've looked at, went from here, then in this direction (indicating)?

A Yes.

Q Around that time and date?

A Correct.

Q Sir, did you also look at the same phone numbers, phone location back on the robbery we've discussed previously, March 4, 2011, Warren, Ohio, around 2:52 p.m?

A Yes.

Q Again, we see the blue square in the middle?

[59]

A Correct.

Q What is that?

A That's the location of the RadioShack at 2553 Parkman Road N.W., in Warren, Ohio.

Q And I see it says Metro PCS and Sprint PCS on the bottom of that charting.

What does that mean?

A The Metro PCS box, the red dots represent the coverage for Metro PCS towers. And the Sprint PCS box represents the coverage for Sprint. It's to illustrate the fact that Metro PCS does not have coverage in the Warren, Ohio area, and that roaming agreement is with Sprint, which does cover that area.

Q Okay. So if you are living in Michigan or Ohio, you probably wouldn't want a Metro PCS phone?

A Michigan, you're okay; Ohio, not so good.

Q But Sprint PCS covers most of Michigan and most of Ohio according to that mapping?

A Yes.

Q So a Metro PCS phone drives down to Ohio, it's going to start utilizing Sprint?

A If you have that agreement with Metro PCS.

Q And is that what occurred here?

A Yes.

Q Okay. And can you tell the jury what you concluded about the location of the 412-6845 phone?

[60]

A There was call activity at 2:12 p.m. and 3:20 p.m. and that -- those calls originated and terminated on tower 208, 293. Again, that 208 represents the equivalent of the area code or the ZIP Code, excuse me. And 293 represents the tower address. And those are represented by the red dot right between the Metro PCS and Sprint insets.

Q I'm seeing it as a blue dot; is that --

A I'm sorry, a blue dot, yes.

Q So it sounds like it was not call activity right at the time of the robbery. There was before and after call activity on this one, right?

A Yes. Those are the two closest calls to the robbery time.

Q And they both show the phone being down by the tower that we can see, which is about how far from the RadioShack?

A I think that was roughly three quarters of a mile to the south.

Q It looks like it's the closest tower to the RadioShack, but it's about a half-mile away that those calls occurred?

A Right.

Q Sir, did you also conduct an analysis of call detail records and phone location for the 412-6845 number for April 5, 2011?

A Yes.

Q And you prepared a chart on that also?

[61]

A Yes.

Q Again, we have the blue square. What is that?

A That is the robbery location of a RadioShack at 14501 Woodward Avenue in Highland Park, Michigan.

Q Okay. And you compared the time of the robbery with some calls that were being made?

A Yes.

Q What did you conclude there?

A Prior to the time on the report which was 2:40, there were two calls, one at 2:21 p.m. and one at 2:30 p.m. The 2:21 call utilized tower 502 and

terminated on tower 170 and 502 is the tower to the bottom represented.

Q Right here (indicating)?

A Yes.

Q So it is within this sector, right?

A Yes. That happens to be a six-sided tower, so the coverage area actually narrows.

Q So this is a little more precise than some of the other towers in terms of sector?

A Yes. We go from roughly 120 degrees of coverage to 60 degrees of coverage.

Q So it's within a more precise sector than some of the others we've been looking at to the RadioShack?

A Correct.

Q And the call lasted 15 minutes?

[62]

A Yes, a little over 15 minutes.

Q Okay. And then it looks like this call is overlapping this call?

A Correct.

Q Can you explain that?

A There is another call that came in and they switched over on call waiting, which created another stamp with regard to what tower was being utilized for that portion of the call, which was on tower -- that call waiting interaction started and finished on tower 502, sector six,

which is the tower to the bottom edge of the map.

Q So the phone on this date and the times shown for the calls was in this sector (indicating)?

A Right.

Q And then the phone moved in this direction (indicating) into the sector up here?

A Well, at the termination of the call, 15 minutes later it was on that sector.

Q Okay. How far is it from here to here (indicating)?

A Roughly a mile, if that.

Q Sir, do you know the general direction of Hamtramck, Michigan from these two towers we're looking at?

A I-75 is running right through the middle of the map so it would be north on 75.

Q Is Hamtramck in this general direction?

[63]

A Yes.

Q Or course, you can't see it on the map, but it's in that general direction?

A Correct.

MR. CHADWELL: That's all I have.

THE COURT: Mr. Gurewitz, would you like to take the morning break now or would you like to proceed?

MR. GUREWITZ: I would. I need to do something here with this equipment.

THE COURT: Very good. So we will give the jury their morning break, okay?

MR. CHADWELL: Yes, Your Honor.

THE COURT: We'll be bringing you out about 20 to 11, okay, 20 to 11.

COURT CLERK: All rise.

(Jury out at 10:19 a.m.)

COURT CLERK: You may be seated.

MR. GUREWITZ: Your Honor, I just wanted you to know that the attorney for the witness I talked about this morning is in the courtroom now.

THE COURT: Yeah. I saw Mr. Kaplovitz the first thing this morning, about 9:00.

MR. GUREWITZ: Yes.

THE COURT: And again, just so the record is -- the witness is who again?

[64]

MR. GUREWITZ: His name is Dewan Taylor.

THE COURT: Okay. And I assume that your expert, Mr. Harmon, has been in the courtroom all morning?

MR. GUREWITZ: He has been.

THE COURT: Okay.

(Court in recess at 10:21 a.m.)

COURT CLERK: All rise.

(Court in session and jury in at 10:48 a.m.)

COURT CLERK: Please be seated.

THE COURT: Mr. Gurewitz, you may start with your cross-examination when you're ready.

MR. GUREWITZ: Thank you.

CROSS-EXAMINATION

BY MR. GUREWITZ:

Q Good morning, Agent Hess.

A Good morning.

Q Forgive me if I missed the description of your background information, but have you had training or experience as an engineer?

A Engineer training?

Q Yes?

A No.

Q What was your college degree in?

A I have a business administration degree for undergrad and a master's in public administration.

[65]

Q Have you taken any continuing education courses related to engineering since you finished your master's degree or left college?

A The extent of my engineering training is through the radio frequency engineers from the cell phone companies.

Q That's sort of on-the-job training. You've had it since you've been working with the FBI?

A Correct.

Q The area that you talked about in a general way to those who don't have knowledge of it may appear to be somewhat technical; is that right?

A Yes.

Q You are familiar with the term also kind of generally from your work on this technical area, luddites. I think it's spelled l-u-d-d-i-t-e-s. I'm not sure if I got it right. Do you know what that means?

A No, I'm not familiar with it.

Q Well, are you familiar with the ways people use words to describe those of us who don't have that kind of technical background?

A I'm not sure what it is that you're asking.

Q Well, I'm just -- there are those people who have technical knowledge and some people don't, right?

A Correct.

Q And that's perhaps why you're here today, because you do?

[66]

A Correct.

Q And please forgive me if I make some mistakes in my questions about some of these technical terms. I'm doing the best I can because I fall in this other category, someone who does not have that kind of experience.

You've had, you said, about 400 hours of training since you have been with the FBI to -- that brings you up to speed to be able to talk

about the things that you've testified about here today?

A Correct.

Q And as a preliminary matter, you know that there are also people who as private consultants are doing similar kinds of advising or providing testimony; isn't that right?

A Sure.

Q Have you met Ryan Harmon in the course of your experience who does private consulting in that area?

A I have not.

Q I'd like to ask you about some of the background information that you testified went into putting together the opinions that you've given today, okay?

A Okay.

Q And just to be clear, when I say opinions, the testimony that you have given here today about the location of cell phones in relationship to particular cell phone towers is opinion, isn't it?

[67]

A Correct.

Q It's not a fact.

A It's based on my training and experience.

Q Right. So we can put information into two different categories. One is factual information, right?

A Yes.

Q And that would be represented in relation to this specifically by the actual records that were obtained from the cell phone companies that indicate the time and number of telephone calls, right?

A Yes.

Q What you have done, also in a general way, is put together that information, arrange it, and done your analysis and to give your opinion; is that correct?

A Yes.

Q Would it be fair to say that in giving your opinion, the kind of opinion that is given is not an exact science, is it?

A What's not an exact science?

Q To reach the opinions that you have given, they're not -- it's not an exact science like a physicist weighing elements or a chemist analyzing the content of something. What you have told us about here is your opinion?

A Right, formulated from my training and experience. Yes.

Q The records that you started out with that have the phone number information are called what?

[68]

A Call detail records.

Q And do you have some of those with you up there today?

A I don't know if they are contained in the exhibit.

Q Oh, the book you have there are the exhibits. Okay.

Well, in a bit, I will show you some examples of those. For purposes of illustration, maybe it would help if I used one now.

What I've shown you, Mr. Hess, is a page from the call detail record relating to this case; isn't that right? Do you recognize that?

A I have no idea if this number is related to this case.

Q Okay. But that is a page that is a call detail record?

A It's an example of one, yes.

MR. GUREWITZ: Your Honor, I represent to the Court that that is part of the records to which we have previously entered in stipulation as to their authenticity. And I move for its admission as Exhibit 2.

MR. CHADWELL: No objection.

THE COURT: All right. Defendant's Exhibit Two is received.

BY MR. GUREWITZ:

Q I'm going to attempt to display this. Here we go.

Agent Hess, could you explain what these columns are in this record? And then I would like to ask you how you use those in putting together your analysis.

[69]

So the first column represents what, please?

A The date of the call.

Q And then we have what, the time of the call?

A Correct.

Q And this column here, the top one, that probably would -- it says "outgoing call"?

A Yes.

Q And that means a call that was made by the particular cell phone?

A Yes.

Q And going across, the next column represents a number. Is that the number of the call?

A It would be the -- I can't see what the column header is. It's that gray area.

Q Okay. Going across this particularly, I want to ask you for the first one at the very top, the last series of columns beginning with where it says "Detroit" and then there are numbers after that, these records are usually set out the same way from Metro PCS when you review them?

A Yes.

Q So "Detroit" is there to signify what, please?

A The market.

Q And then the number signifies what about the market?

A Whether it's market one or market two in Detroit.

Q And does that indicate which tower is used?

[70]

A It represents a geographic area of the state.

Q What about the number 117?

A One-seventeen is the tower that's used. It's a cell site identifier.

Q All right. Is there anything there to indicate with regard to the cell site and the particular tower? You talked about antennas. Which antenna was used on the tower?

A The comma between where it says "Detroit one" and "117," the number two represents the sector.

Q Now, this is an example of one of the pages from the records that were made available. Did you do anything to obtain these records yourself?

A No.

Q In this case?

A No.

Q They were provided to you?

A Correct.

Q Did you indicate to Agent Ruiz then what records you thought were necessary for you in order to perform your work?

A Yes.

Q Would it be fair to say that when you did this analysis then, the records go in chronological order; is that right?

A Yes.

Q And they then would list or they should list all the calls that were recorded by the cell phone company for the [71] particular phone during the time period that is represented in the records, right?

A Yes.

Q It would show calls that were in this category of made and received, right?

A Yes.

Q And calls that are call waiting?

A Correct.

Q And based upon your experience, what does that mean?

A That's another call that is received.

Q And these records then recorded the same kind of information, don't they, for a call that is a call waiting, that is, it shows the tower that was used and the particular antenna; is that right?

A Yes.

Q Is that something that you had an opportunity to look at doing your analysis?

A There was an instance of a call waiting.

Q Well, there's more than one, in fact, wasn't there?

A I don't know that there was, but with regard to the dates and times I looked at there was one instance.

Q Yeah. It was part of what you did to determine from all of these calls which ones were relevant

to the opinion that you were asked to give; isn't that right?

A I looked at the calls as close to the robbery report time [72] as were available on the records.

Q You looked at all of the ones that were close to the time that was available on the record; is that your testimony?

A Yes.

Q You have given testimony here about this exhibit that is part of I believe, 57.

MR. GUREWITZ: Is that correct, Mr. Chadwell? Is that the number here?

MR. CHADWELL: Yes.

BY MR. GUREWITZ:

Q You created this; is that right?

A Yes.

Q Did you use some kind of -- tell me what your technique was for preparing this.

A The cell phone company provides a list of where their tower locations are.

Q Was that included in this example, the call data report page that I showed you?

A No.

Q How was that obtained?

A Through legal process; search warrant, court order.

Q Did you obtain those records for your use in connection with each one of these documents that you prepared?

A Yes.

Q And just so I understand how to refer to this, what I [73] have exhibited right now is one of these pages for December 13, 2010.

What do you call this page? Is it a map or something else?

A It's a map, a demonstrative.

Q Okay. What else do you use in order to create this map, the one that's displayed here for December 13th?

A The call detail records are provided in electronic format in an Excel spreadsheet. The mapping software is Microsoft MapPoint. The call detail records are utilized and the tower list is utilized.

Q Are you familiar with a program, software called Pen-Link?

A Yes.

Q What is that?

A Pen-Link is an analytical tool with regard to cell phones.

Q And did you use that in connection with the creation of these maps?

A I did not.

Q Then how did you actually create the map that shows the specific location of the towers on the map? How did those get put on there in the places that they appear?

A There's an import function in the Microsoft mapping software that allows you to import a data set based on in [74] this case the tower latitude and longitude.

Q So the information that you're talking about that you received from the cell phone companies that allowed you to locate them is something that lists the kind of map coordinates that we hear about longitude and latitude for each one of these towers?

A Yes. They provide a physical address, as well as a latitude and longitude.

Q With regard to each of these towers that you have identified on this one that's up there right now for December 13, for example, there are sectors that pertain to each tower; isn't that correct?

A Yes.

Q Is that important to you in your work, what the sectors are?

A Yes.

Q Why is that?

A Because they tell you the side of the tower that was utilized for a particular call.

Q And the number of sectors on the tower depends on the number of antennas on it; is that right?

A It depends on whether it's oriented to a three-sided or a six-sided tower.

Q When you're talking about sides of the towers, really what you get to is the antenna is the

significant part, [75] because that's where the signal from the phone is either received or sent to, right?

A Yes.

Q There are some towers that are three and some that are six?

A And some that are one, yes.

Q Have they all been regularly divided into equal parts of a 360-degree radius?

A I can't say that all are, no.

Q Some vary, don't they?

A Yes.

Q And how do you take that into consideration when you're doing your work?

A I look at what is called the beam width.

Q The what?

A The beam width.

Q Is that information something that also came to you to do your analysis here?

A And the tower list.

Q Now, you talked about a number of things that affect which towers' signal from the phone might reach. There are a lot of factors, aren't there?

A Sure.

Q And those include things that you talked about, such as the -- whether it's a mountainous area or a flat area that [76] the tower is located in?

A Yes.

Q And whether there are high buildings or not in a particular area?

A Yes.

Q It also includes things that relate particularly to the functioning of individual cell phones, such as the strength of the battery in a particular phone; is that right?

A Yes.

Q How would that affect a selection by the phone of the tower which is going to be used to send or receive a signal?

A The power management of the phone is relying on the amount of power that's still remaining in the battery.

Q So if the phone has a weak battery, it would have to be closer to a tower than one with a strong battery?

A Not necessarily.

Q Okay. That varies, too, depending on other circumstances, right?

A Yes.

Q And another factor that affects the distance is the weather; isn't that right?

A To some degree, yes.

Q Well, to the extent it does, the temperature might make a difference?

A Yes.

[77]

Q And things that are going on relating to some activity or something like that, I don't know the term, might make a difference, interference in the air?

A Yes.

Q The amount of activity that is going on at a particular time when the call is made might also affect which tower is used; isn't that right?

A No.

Q Well, if a call is made at between the hours of four and six in an urban area where a lot of people are driving and probably using cell phones when they shouldn't, there's a lot of activity.

Wouldn't the congestion of -- I'm using the word "congestion," but the amount of activity and phone calls at that time affect the availability of which tower would be used?

A The phone number doesn't know what the volume is on the tower.

Q But towers have limits on how much reception they can provide; isn't that right?

A For traffic channels?

Q Yes.

A Yes, it has limits.

Q So one of the factors then that comes into play because of all of those things which you just testified about as [78] variables that affect this

is the relationship between a tower and an adjacent tower; isn't that right?

A Yes.

Q Why is that?

A Because it affects the coverage area of each tower.

Q In what way?

A Well, if the cell sites are a mile apart versus five miles apart, the coverage area would increase or decrease based on proximity.

Q So it does happen sometimes that a phone call that's made can shift from one tower to another while the call is going on, right?

A Yes.

Q And that can happen because the cell phone moves, right?

A Yes.

Q And it can happen because of some other variables that might be included in the things that you've just testified about, right?

A Yes.

Q And when I asked you early on in the questions I was asking you this morning about whether all of this is an exact science, one of the reasons it's not an exact science is because some of these things you really can't actually determine when you're just looking at records on paper; isn't that right?

[79]

A What things?

Q Well, for example, the variables, such as weather conditions and the battery strength, right?

A Yes.

Q But you should be able to take into account the relationship between a tower and an adjacent tower; isn't that right?

A Yes.

Q On this map for December 13th, how many towers did you identify by number on that map?

A There is three towers.

Q And there is one identified down here at the bottom, that's 127; is that right?

A Correct.

Q And there is one up here, 145?

A Yes.

Q And there is one over here that's on a -- looks like it's on the edge of the Ford Expressway, that is 164?

A Right.

Q That's three?

A Yes.

Q What are those other red dots there?

A Other towers for Metro PCS in the area.

Q You made a decision not to attach numbers to those?

A Those towers were not utilized with regard to the call [80] detail records.

Q Because they didn't relate to the two calls that you chose to put up at the top of this map, is that right?

A Right.

Q When you talked about a place where a phone was located at the time of the call, are you referring to what you mentioned as a service area?

A Yes.

Q And can you describe then what a service area actually is for the ladies and gentlemen of the jury?

A For illustration, if defense counsel's podium is your cell site and it's broken into three sectors. the gallery would be a sector, that area to the back of the room would be the service area. To the jury box side, service area, to the defense side, service area.

Q Except, in fact, these service areas aren't the size of 15 to 20 feet, are they?

A No.

Q You just did that for an illustration, right?

A Correct.

Q What would be the physical layout of this? How much distance would be taken up by that?

A It would be based upon proximity to other towers.

Q Okay. So in this case it might depend upon the proximity of the three towers you have located there to the other [81] towers that you don't have numbers for, right?

A Yes.

Q Can you give us some range of what these physical distances in terms of mile, half-mile; how big would those areas be?

A Well, in Detroit, based on my experience, I have seen anywhere from a half-mile coverage to a little over two mile coverage.

Q When you talk about that, what comes to mind is you're talking about a straight-line at the half-mile, but the service area is not just a straight line. It's like sort of a wedge or a pie shape?

A Yes.

Q And it would be narrowest obviously then when it gets to the tower, but when you get out to the edge of it, how big an area would that be? If it's a half-mile to a mile in distance, the part that connects these two spokes of this would be how far apart, mile, mile and-a-half?

A Roughly.

Q So that when you talk about location, a call during a particular time that you have plotted on these maps, you are not saying that the call was, for example, in a parking lot at the corner of Freud and -- well, that doesn't run that way.

Well, Jefferson and Newport, for example, streets [82] that intersect, you are not able to

say that the phone was at a particular place, right?

A Correct.

Q What you would really say at best is that it is somewhere within that area that could be a-half mile to a mile in distance from the tower and then connecting those two, right?

A Right. As well as where the phone isn't.

Q What do you mean by that?

A Well, in previous cases, alibis have been offered and alibis are not found at times, that this would disprove an alibi. So in other words, if we were using those towers and there was an alibi that was provided that the individual was in Harper words, it's not possible to be using those towers while in Harper Woods.

Q But that doesn't really relate to what you're talking about in terms of placing a call within a service area, this pie-shaped distance, a-half mile to a mile out from the tower.

What you're saying is that you've made a determination that a call was at some point in time in that service area, right, when you locate it there?

A Exactly, yes.

Q Okay. Could you have been more precise in your measurement if you had taken into consideration the adjacent towers and factoring in their service area?

[83]

A Well, I didn't measure what the distance is of the coverage area. I simply illustrated what side of the tower was utilized for that call.

Q So you have really not given the jury here today any opinion about exactly where a phone was at any particular time, have you?

A The exactness of it would be within the footprint of that tower on that sector.

Q But more specifically than that, you haven't given us any opinion about where it could have been within that area, right?

A Right.

Q And another thing that you can't do through this analysis in any way at all is to tell us anything at all about who was actually using the phone at the time that the call was made, right?

A Correct.

Q This all is just based upon the abstract, cold analysis of records that come from the phone company and the location of cell towers?

A I wouldn't classify it as abstract.

Q Let me ask you some more specific questions then.

You have used these call data records that are in your work referred to by initials as CDRs?

A Yes.

[84]

Q To list information for a call that was at 10:24 a.m. and had a duration of about four minutes?

A Right.

Q And that originated on tower 127, sector one?

A Yes.

Q And I'm not sure. Is that the one I am pointing to right now?

A Yes, it is.

Q And according to this record, the call terminated on sector two, and that's the one below; is that right?

A The box is below, but it's to the right?

Q The box is below, but both those boxes pertain to the same tower, right?

A Yes.

Q And sector one and sector two then that designates the direction of this particular service area that goes out from that particular cell tower, right?

A Yes.

Q Could you tell us, please, then what those directions are for this particular tower?

A On the bottom of the box you see "ANT orientation." That's antenna orientation. And the number is what's called the azimuth or the point on a compass, the degree point on a compass. So the 1271, the azimuth is zero, so the center of that sector points to 12 o'clock.

[85]

Q Now, is this little piece of plastic I'm holding up an azimuth?

A It's a protractor.

Q A protractor, okay.

Does that help you describing the directions you are talking about?

A A clock works just as well.

Q Okay, there's one up on the wall.

So for the first call that you're talking about here, what is the direction from this tower of the relationship of that call, according to your analysis in that tower?

A Towards 12 o'clock.

Q Twelve o'clock would be as I'm holding the pen straight up, vertically; is that right?

A Yes, that's the azimuth.

Q And by "azimuth," do you mean that the call, according to your analysis, was directly on that line, going vertically from that tower?

A No.

Q What do you mean?

A I mean the sector is based off the azimuth, so if it's 120 degrees, we'll go 60 degrees to the left, which would bring you to ten o'clock on a clock; 60 degrees to the right, which would bring you roughly to two o'clock.

[86]

So somewhere within ten to two is where that device was at the time of that call.

Q And the second part of that call was on sector two. And what's the azimuth for that?

A Eighty.

Q Could you explain what that means here physically, what direction?

A Three o'clock would be 90, so 2:30 on a clock.

Q Is that pointing off to the right side of this map from that --

A Yes.

Q Does that indicate that during the time period of this call that there was movement in the location of the phone in relation to the tower?

A Potentially.

Q That's a possibility, isn't it?

A Certainly.

Q And you can't say that it was or it wasn't?

A Right.

Q It could have shown a different sector because of a whole bunch of variables, right?

A Sure.

Q Now, I would like to show you again Exhibit Number Two.

Hopefully, I can put this up so we can all see it. And there is a call there on 12/13/2010 at 10:31:21.

[87]

Do you see that?

A Yes.

Q Is that call on your map?

A These are not records that I analyzed, so it wouldn't be on that map.

Q They are not records you analyzed?

A No. Those are records for a different telephone number, if that's what you showed me before.

Q I think it is.

MR. GUREWITZ: Just a moment, Your Honor.

THE COURT: Members of the jury, I guess we're going to go up to 2:45 today as we discussed yesterday. And I will be giving you a lunch break probably at about at 12:45 to 1:30. Okay?

MR. GUREWITZ: All right, I apologize.

BY MR. GUREWITZ:

Q Let me show you what I have marked as Exhibit Three.

Does that appear to be a CDR, call detail record for the number that you examined?

A Yes.

Q Okay. And that pertains to the date of December 13, 2010?

A Yes.

Q That is a page that you did examine?

A Yes.

[88]

Q Thank you.

MR. GUREWITZ: Your Honor, I'd move for its admission.

MR. CHADWELL: No objection.

THE COURT: All right. Defendant's Three is received. And that's the call record for December 13, 2010?

MR. GUREWITZ: 12/13/2010.

BY MR. GUREWITZ:

Q I'd like to direct your attention to the top -- the top two lines are the ones that you have listed on your map; isn't that right?

A Yes.

Q Right below that, there are two calls, one at 10:36 and one at 10:37. Do you see that?

A Yes.

Q The information on the last column shows the towers that were used for these calls; is that right?

A Yes.

Q The second call was to -- the second one that you have on your map, shows that the beginning tower was 145 and the ending tower was 164?

A Right.

Q And then for the call immediately below it, the beginning tower is 469 and ending is 164; is that right?

A Yes.

[89]

Q And the one below that starts at 164 and ends at 168; doesn't it?

A Correct.

Q Did you determine the location of those two other towers on your map?

A I did not.

Q These records for calls that were placed or were in existence at 10:36 and 10:37 indicate that there was movement of the phone during that time period; isn't that right?

A Potentially.

Q But that is one possibility, right?

A It could be movement of two feet.

Q Of what?

A It could be movement of two feet versus six blocks.

Q You don't know that at all though, do you?

A No. Not with regard to that, no.

Q The only thing that is really fixed in your analysis that you know for sure is the location of the tower; isn't that right?

A Yes.

Q According to these records and the movement, it is entirely possible that the phone was moving up Jefferson Avenue during extended time from 10:24 through 10:37; isn't that right?

A Sure it's possible.

[90]

Q You can't say with any certainty whether the phone was north or south of the RadioShack store at the time of the robbery, can you?

A No.

Q I would like to ask you some questions about your testimony concerning the map you created related to December 18, 2010.

In your review of the CDRs, the usage records for the phone that you examined, looking for the particular date of December 18, 2010, did you find that there was frequent usage by that particular phone number of the towers that you've identified here, 173, 186 and 188, during the month of December of that year?

A That wasn't the source of my analysis, no.

Q What wasn't the source of your analysis?

A The count call frequency or tower frequency.

Q Oh, you mean it wasn't what you were asked to do?

A Right.

Q Okay. Just a moment.

Now, Agent Hess, if, in fact, there was a pattern of usage by this particular number that you were examining records for, only for the date of December 18, 2010, of those towers from December 1st through December 18th, using the same towers, would that indicate that that phone was someone who lived in that particular

A Yes.

[89]

Q And the one below that starts at 164 and ends at 168; doesn't it?

A Correct.

Q Did you determine the location of those two other towers on your map?

A I did not.

Q These records for calls that were placed or were in existence at 10:36 and 10:37 indicate that there was movement of the phone during that time period; isn't that right?

A Potentially.

Q But that is one possibility, right?

A It could be movement of two feet.

Q Of what?

A It could be movement of two feet versus six blocks.

Q You don't know that at all though, do you?

A No. Not with regard to that, no.

Q The only thing that is really fixed in your analysis that you know for sure is the location of the tower; isn't that right?

A Yes.

Q According to these records and the movement, it is entirely possible that the phone was moving up Jefferson Avenue during extended time from 10:24 through 10:37; isn't that right?

A Sure it's possible.

[90]

Q You can't say with any certainty whether the phone was north or south of the RadioShack store at the time of the robbery, can you?

A No.

Q I would like to ask you some questions about your testimony concerning the map you created related to December 18, 2010.

In your review of the CDRs, the usage records for the phone that you examined, looking for the particular date of December 18, 2010, did you find that there was frequent usage by that particular phone number of the towers that you've identified here, 173, 186 and 188, during the month of December of that year?

A That wasn't the source of my analysis, no.

Q What wasn't the source of your analysis?

A The count call frequency or tower frequency.

Q Oh, you mean it wasn't what you were asked to do?

A Right.

Q Okay. Just a moment.

Now, Agent Hess, if, in fact, there was a pattern of usage by this particular number that you were examining records for, only for the date of December 18, 2010, of those towers from December 1st through December 18th, using the same towers, would that indicate that that phone was someone who lived in that particular

area and had a reason to be [91] there on a regular basis?

A Potentially.

Q So that your analysis doesn't determine why someone is there, why a phone is in a particular place, only that it was at the specific narrow time that you were looking at; is that right.

A Yes.

Q In your analysis to determine -- to investigate the range of criminal activity that you're talking about, is it sometimes your practice to attempt to exclude other possible reasons with regard to phones, that a phone is in a particular location, only that it is associated with a fact that you are investigating?

A Yes, I've used it to include and exclude, yes.

Q And that's a fair thing to do as an investigator, isn't it?

A Yes.

Q You don't typically, as an investigator -- as an FBI agent, you weren't trained just to go out and prove something that somebody else told you happened, right?

A Right.

Q Your job is to examine all the facts, isn't it?

A Correct.

Q But here, all you did was look at the CDRs for one day, right?

[92]

A Because that is what I was asked to do.

Q And who asked you to do that?

A Agent Ruiz.

Q But as an expert in this area providing assistance to the FBI, did you say to him, "Agent Ruiz, maybe it's possible that this phone frequently is in this area and uses the tower at the same times on other days of the week, on other weeks of that month? Shouldn't we look at that?"

Did you say that to him?

A It doesn't exclude the fact that criminal activity could have taken place.

Q But it would have raised some real questions about it, wouldn't it have?

A Not necessarily.

Q But it could have?

A It could have.

Q Do you have within this judgment call that you make on these locations then, for placing a phone call at a particular time within a particular area, do you have a range of certainty that you want to be able to meet in order to reach a conclusion?

A I'm not sure what you are referring to as a "range," sir.

Q You have given us a lot of reasons why it would appear that these determinations you make are not an exact science, right?

[93]

A Right.

Q How comfortable do you need to be with this before you create a report with an opinion on it?

A Based on my training and experience, I'm comfortable in generating the report.

Q Now, what I have displayed now is the map that you have created for March 4, 2011. It says at 2:52 p.m. -- and you have given testimony about review of records. One thing I noticed about this is that you don't have any call information at the top of this map; isn't that right?

A Right.

Q On all the other ones you do?

A Yes.

Q This map pertains to an area where there isn't Metro PCS coverage; isn't that right?

A Right.

Q And you've got the Sprint coverage area depicted down in the bottom with a little box in blue?

A Yes.

Q And for most of that area that shows Michigan, it's just sort of a solid mass of colors of blue.

Is this supposed to represent individual dots that would be cell towers?

A Yes.

Q Where did you get that information?

[94]

A From Sprint.

Q Did you use a court order to do that?

A No, I did not.

Q Where did it come from exactly, how did you get it?

A We have records from prior cases.

Q So based upon these other records -- that's what you, in fact, used, records from other cases?

A I don't recall if I used records from other cases or if Agent Ruiz had furnished the tower list for Sprint.

Q You don't have a present memory now of exactly what you did in order to place the tower information location into your map, right?

A I don't recall if it was an existing tower list already in my possession or if it was one that was provided by Agent Ruiz.

Q Do you have that somewhere in your records that you looked at in preparation for your testimony for today?

A Do I have it somewhere?

Q Yes.

A Yes. I created a map as a result of it.

Q Okay. But it's based upon those records that you placed in the tower where it is represented by that blue dot?

A Yes.

Q And according to your map here, this shows information here that is tower 293; is that correct?

[95]

A Yes.

Q This first number 200 -- I can't tell if it's 200 or 206 or 8.

A Two hundred and eight.

Q That represents the region?

A Yes. Sprint calls it a REPOLL number.

Q What is a REPOLL, R-E-P-O-L-L?

A As I had explained earlier on the T-Mobile, we have the location area code. It's the equivalent of a Zip Code. It puts you in a geographic region of the country.

Q So that's a much bigger area than what is depicted by this particular map, isn't it?

A Well, there would be numerous cell sites within REPOLL 208.

Q The most specific, narrow identification you have here for the coverage of this tower is what number?

A The 293.

Q Where is the information that describes the sectors for this antenna?

A It's the first digit before the 293.

Q And what is that?

A The box on the left I believe is a one. The box on the right is a two.

Q Do you have that? Maybe it doesn't come through clearly on the projector here. Do you have that in front of you?

[96]

A Yes.

Q Could you point that out exactly where those numbers are?

A Sure. It's 208, one; 293, 208, two -- or excuse me, three, 293.

Q Okay. Now then, tell us please what is the orientation of those antennas and which way do the sectors face that you have plotted out there?

A I didn't include the antenna orientation.

Q Is that information shown?

A No.

Q Did you obtain it from Sprint?

A I'm sure it's in the tower list.

Q I'm sorry?

A I'm sure it's in the tower list.

Q Would that have been included -- was it included for the other maps with the call information that you placed at the top of the pages?

A It was.

Q Is there some reason you left it off here?

A Because I was satisfied that the fact that it was in Warren, Ohio in proximity to the RadioShack was sufficient.

Q So that your purpose in doing this one was only to show that this was in Warren, Ohio, right?

A Correct.

Q And that's all you have shown here?

[97]

A Yes.

Q And your opinion only establishes that these phone calls were in Warren, Ohio, right?

A In close proximity to the robbery location.

Q Well, just to be specific for the record, at the present time you don't know whether that's north, south, east or west of this road down here that the tower is adjacent to; is that right?

A Well, based on?

Q Based upon your analysis of the records, you can't tell.

A Well, I can tell you based upon the map that sector one would be to the north.

Q And you don't know how big that sector is at all, right?

A No.

Q Now finally, I would like to direct your attention to the date of April 5, 2011, okay?

First of all, I'll ask you a question about geography in that phone usage. The location of

Hamtramck -- how long have you lived in Michigan?

A I can cut you off here. Hamtramck is due east. I misspoke earlier.

Q And it's south of the Davison Expressway; isn't it, primarily?

A Yes.

Q So if the phone calls that you have analyzed here showed [98] movement from the tower that's down in the lower part that I'm pointing to at the bottom of the page, up to the direction of the tower that is north of the Davison Expressway and east of I-75, that's not going toward Hamtramck, is it?

A Right. Now that I'm oriented, no, it's not.

Q In this case which you have shown is that a call -- the time of the robbery up there is 2:40; is that right?

A Yes.

Q By the way, with each of these maps, where did you get the time for the robbery?

A That's based on the police report.

Q Is it generally your understanding from your experience in doing this kind of work, that's not an exact, precise time either, is it?

A I'm not sure how it wouldn't be the precise time.

Q The time that the police would have, is it at the time it's reported, the time it occurred or what?

A It's not going to be the time that it occurred, because that would suggest that somebody was

standing right there and dialed 911 as the robbery is happening.

Q So it could?

A But at the time of the call being entered into the dispatch system, there could be an offset of from the time of the actual occurrence of the robbery to the time that it's [99] entered in the system.

Q So it's generally your view that at the time the robberies that are used for these maps are the times that are recorded in police reports for when they were reported; is that right?

A It's what's generated on the police report. I don't know the practice of the individual agencies.

Q In this case, the first call that you have plotted out here is at 14:21 and 43 seconds. Is that right?

A Yes.

Q And it has a duration of how long?

A Fifteen minutes and 23 seconds.

Q So that would take it from almost 14:22 to almost 14:38?

A I'm sorry?

Q It would take it from -- 14 is two, 2:21 and 43 seconds, p.m., right?

A Yes.

Q It would take it to its ending time at almost 2:38 p.m., right?

A Right.

Q Now, the second call is one that shows it incoming?

A Yes.

Q And this one is a call waiting, right.

A Yes.

Q You put a call waiting call on this one, didn't you?

[100]

A Yes.

Q So in this case, you found it to be important enough for you to put down on your map?

A Because it was immediately prior to the robbery report time.

Q And how long does this one last?

A Eighteen seconds.

Q The tower location goes from starting with 502 to 170, right?

A Yes.

Q And where are those towers located on your map?

A The 502 is the tower at the lower portion of the map and 170 is the one that's about dead center on the map.

Q Does someone need to answer an incoming call while they're on the phone in order for it to be registered as call waiting?

A That shows that it was answered.

Q Okay. Was it your testimony before in connection with identifying Hamtramck that there in this case was some indication of movement during this call?

A Yes. At some point, yes.

Q And what do you mean by that? What would be the direction of the movement?

A Well, exact direction of movement, I can't say. At the time of the termination of the call it was on tower 170 in [101] the middle of the map. How they got to 170 from 502, I don't want to --

Q This is 170, you said middle of the map. It's up in the right-hand quadrant of the map, right?

A Yes.

Q And again, this wider depiction of the road here is the Davison Expressway?

A Yes.

Q So it's a limited access road; isn't that true?

A Yes. There's entrance and exit ramps.

Q The direction then -- these two lines up here on the top, are those put there by you to indicate the direction of this particular service area or sector that you determined that the call was within?

A Yes. To illustrate the orientation.

Q So that on the first call, it was within this pie-shaped area designated by these two lines down here and up there.

It's within those two, right?

A Yes.

Q And it's clear then, according to your analysis that that phone in whatever way moved from within that small sector in the lower part, up to the one at the top, right?

A Fifteen minutes later, yes.

Q And that the time again for that movement was from 14:21 until about 2:31, right? Is that -- that's not right because [102] that call waiting call happened during the first call?

A Yes.

Q So the second call ended at what time?

A The second call ended at 14:30:28, 18-second duration.

THE COURT: Mr. Gurewitz, could we take about a five-minute break right now?

MR. GUREWITZ: Sure. I'm almost done, but this is fine.

THE COURT: Okay. Members of the jury, I guess at least one of you needs a little recess, so we're going to have you go back to the jury room for about five minutes and then we'll bring you right back out, okay?

COURT CLERK: All rise.

(Jury out and Court in recess at 11:50 a.m.)

(Court in session at 11:58 a.m.)

THE COURT: Okay, back on. We've had a discussion regarding the jury instructions. I think everyone is in agreement as to the jury instructions, the

jury instructions that will be given to the jury, except there's two issues.

There's the venue jury instruction, as well as what jury instruction will be given under aiding and abetting the gun charge; is that correct?

MR. CHADWELL: Yes, Your Honor.

MR. EARLY: Yes, Your Honor.

MR. GUREWITZ: Yes, Your Honor.

* * * * *

[105]

THE COURT: Mr. Gurewitz, you may continue when you're ready.

MR. GUREWITZ: Thank you.

THE COURT: Counsel, just be a little bit careful when you're having stuff put up on the screen, so that you're not standing in front of the screen.

MR. GUREWITZ: I'm sorry.

THE COURT: I'm not saying you, just in general. Just be careful you're not blocking the projector.

MR. GUREWITZ: I apologize.

THE COURT: I didn't say it was you, Mr. Gurewitz.

BY MR. GUREWITZ:

Q Agent Hess, just the last topic and a couple of questions I have about this exhibit or just about the time of these calls again and where they went. They start at 2:21, right?

A Yes.

Q And they go until about 2:36, right?

A Yes.

Q Maybe 2:37.

And they move from -- I'm not going to stand in front of the screen this time -- the bottom up to top, from the bottom part by the expressway over to that red circle which is the tower on that upper right side, right?

A Yes.

Q And according to your lines up there that mark out where [106] that sector was, the call was within that top sector at about the 2:36 time, right?

A Yes, at the termination point. Yes.

Q And according to the information that you got from Agent Ruiz, this robbery happened at 2:40?

A Correct.

Q Now, you talked before that sometimes you have to take into consideration in what you do, things like alibis, I think?

A Yes.

Q Well, in this case, the information that you got to take into consideration was that a robbery took place at 2:40 p.m., as of the best time that you were able to obtain from Agent Ruiz, correct?

A Correct.

Q And that this investigation pertaining to Mr. Carpenter was about whether or not he was

acting as a lookout for the robbery that happened at 2:40 p.m; isn't that right?

A That I don't know.

Q That wasn't at all a factor in your putting together this work? You didn't know that information?

A No. I simply looked at where the location of the telephone was at the time of the call?

Q What you found was that the information showed that there was movement from the location of the bottom tower up to this [107] one that is northeast of the Davison -- north of the Davison Expressway and East of I-75 before the time that this robbery took place; isn't that right?

A No.

Q Well, the ending time of that call is at 2:36, isn't it?

A Correct.

Q And the robbery, according to this, is at 2:40?

A Correct.

Q So that the location of the phone at 2:36 was in that sector, this tower over here, 170, facing north, right?

A Yes. However, at 2:30 it was in the tower south of the robbery location.

Q At 2:30? That's ten minutes before the robbery, right?

A Yes.

Q And at four minutes before the robbery, it was north of that tower 170.

A I'm sorry, at four minutes before the robbery?

Q Three minutes before the robbery, 2:37.

A Before the report time.

Q I'm sorry?

A Before the report time.

Q Before the -- whatever that is, right?

A It could be three minutes after the robbery.

Q You don't know that, do you?

A Exactly. Neither do you.

[108]

Q But that is something that you can say exactly, is that you don't know?

A Yes.

Q All right. The last thing I want to ask you, just go back briefly to ask you maybe just one question, that April -- excuse me, March 4, 2011, you said that what you -- your source of information for the location of the Sprint towers was data that the FBI had from other cases; is that right?

A Yes.

Q It is true, isn't it, that cell tower locations vary, right? They are not always the same?

A In what way?

Q Well, sometimes you don't know when cell towers are created, right?

A Correct.

Q Do you know what the date of the data was that you looked at for this purpose from Sprint?

A I don't recall the exact date, but it would be a date going back to that time frame of 2011.

Q But you don't recall the exact date?

A No.

MR. GUREWITZ: That's all I have at this time, Your Honor.

THE COURT: All right. Mr. Early?

MR. EARLY: Thank you.

[109]

CROSS-EXAMINATION

BY MR. EARLY:

Q Good afternoon, Agent Hess.

A Good afternoon.

Q I represent Timothy Sanders.

And I want to talk to you because you have already talked about the other robberies in Detroit, those maps which don't involve my client.

So I want to talk to you about a robbery that occurred in Detroit on January 7, 2011 which my client is charged with, okay?

A Okay.

Q And as I understand it, you did not obtain any cellular phone data or what you call call data reports for January 7, 2011, did you?

A None were furnished to me, no.

Q Okay. And you were advised there was a robbery on January 7, 2011; is that correct?

A Maybe. I don't know what the robbery dates were.

Q Well, did you do this chart here that says "T-Mobile robbery January 7, 2011, no cellular phone data"?

Do you want me to come closer and give it to you?

A Yes. I don't know what you're referring to.

Q I received this, I represent to the Court, along with your maps and other things, just this sheet of paper saying [110] "no cellular phone data for 2011."

Do you remember that?

A I can't say that -- that I created that slide.

Q But you do know that there's no data?

A I can't tell you that and I agree, I don't know that I created that slide.

Q But you do know that there's no data for January 7, 2011 though, right?

A There was no data on the records that were provided to me.

Q Okay. And obviously you were told something about January 7, 2011 because you know that there's no data for that date, right?

A Yes.

Q Okay. And the thing you were told is that there was a robbery that date. "We want you to analyze that." And you said "There's no data," right?

A I can't characterize it, what was stated?

Q Now, did you ever ask Mr. Ruiz for the data for January 7, 2011?

A No, because I was asked to analyze March 4th.

Q And I'm asking you, did you ever ask Mr. Ruiz for data for January 7, 2011?

A And I answered, no.

Q Okay. So we don't know on the basis of your examination [111] where the phone number belonging to Big Tim on this chart, 579-8507, was on January 7, 2011, do we, because you've done no analysis?

A Correct.

Q Now, I just have one question or two regarding March 4, 2011, which is an Ohio robbery. Do you remember that one?

A Yes.

Q Okay.

MR. EARLY: And may I have just one moment, Your Honor?

(Pause in proceedings)

BY MR. EARLY:

Q So are you telling us you never talked to Mr. Ruiz about January the 4th -- January 7, 2011?

A I can't say that I have or I haven't. I don't recall.

Q You don't recall?

A No.

Q Is there anything that would refresh your recollection as to whether or not you discussed January 7, 2011 with Mr. Ruiz?

A I can't say that there is or there isn't.

Q Now, in your report, you have on page -- you have the report up there in front of you, don't you?

A Yes.

Q On page two of your report, you say the purpose of the [112] analysis; is that correct?

A Correct.

Q And you say Special Agent Ruiz requested cell site analysis of the target phones to determine the geographic area where the target phones were located in relation to incident dates and times; is that correct?

A Yes.

Q And you're saying you don't remember anything that he supplied you about January 7, 2011?

A That's what I'm saying, yes.

Q And did you look at the call detail reports for telephone number 8507?

A Yes.

Q And isn't it a fact that the call detail reports for 8507 start at January 17, 2011?

A I would have to look at the actual records.

Q Here they are. Take a look.

A Can you point me to the page that it's on?

Q It starts at page one. That should be the one that --

MR. CHADWELL: Your Honor, I think this is inappropriate. Here he's handed the witness a stack of about a foot of paper.

MR. EARLY: I'll show him, Your Honor.

MR. CHADWELL: The witness has already clearly said he had nothing to provide on that date. And so I think from [113] here on out, he's just harassing the witness.

BY MR. EARLY:

Q I'd ask you to look at the first page here. What's the top sheet?

THE COURT: Wait, just -- what's the question?

BY MR. EARLY:

Q Okay. Are these the call details, Officer, for 8507; do they look familiar to you?

A Yes.

Q And what is the first date here that is reported to you on the call detail records?

A January 17, 2011.

Q Do you see January 7, 2011 on there, sir?

A No.

Q Thank you. And did you ever bother to ask Ruiz for January 7, 2011?

MR. CHADWELL: Asked and answered, Your Honor.

THE COURT: I think he said he didn't recall.

BY MR. EARLY:

Q You don't recall or is it a no?

A He provided me with the records that he had in his possession.

Q So did you ever ask him for January 7th?

A No.

Q Now, let's go to March 4, 2011. Now, as I understand it, [114] you're saying -- this is the analysis of -- you have it there, don't you, Mr. Hess?

A Yes.

Q You have this document, don't you?

A Yes.

Q Okay. This is March 4, 2011, 2:52. You are analyzing which you say is the report time for the robbery; is that correct?

A Correct.

Q Okay. Now at that time you're saying that the phone number of 8507 is there where that red is; is that -- that the tower location -- it's pinging off that tower where the red is? Is that you're saying, basically?

A Yes.

Q Okay. So you're saying that the phone is located over there somewhere by that tower; is that basically what you're saying?

A Yes.

Q Here they are. Take a look.

A Can you point me to the page that it's on?

Q It starts at page one. That should be the one that --

MR. CHADWELL: Your Honor, I think this is inappropriate. Here he's handed the witness a stack of about a foot of paper.

MR. EARLY: I'll show him, Your Honor.

MR. CHADWELL: The witness has already clearly said he had nothing to provide on that date. And so I think from [113] here on out, he's just harassing the witness.

BY MR. EARLY:

Q I'd ask you to look at the first page here. What's the top sheet?

THE COURT: Wait, just -- what's the question?

BY MR. EARLY:

Q Okay. Are these the call details, Officer, for 8507; do they look familiar to you?

A Yes.

Q And what is the first date here that is reported to you on the call detail records?

A January 17, 2011.

Q Do you see January 7, 2011 on there, sir?

A No.

Q Thank you. And did you ever bother to ask Ruiz for January 7, 2011?

MR. CHADWELL: Asked and answered, Your Honor.

THE COURT: I think he said he didn't recall.

BY MR. EARLY:

Q You don't recall or is it a no?

A He provided me with the records that he had in his possession.

Q So did you ever ask him for January 7th?

A No.

Q Now, let's go to March 4, 2011. Now, as I understand it, [114] you're saying -- this is the analysis of -- you have it there, don't you, Mr. Hess?

A Yes.

Q You have this document, don't you?

A Yes.

Q Okay. This is March 4, 2011, 2:52. You are analyzing which you say is the report time for the robbery; is that correct?

A Correct.

Q Okay. Now at that time you're saying that the phone number of 8507 is there where that red is; is that -- that the tower location -- it's pinging off that tower where the red is? Is that you're saying, basically?

A Yes.

Q Okay. So you're saying that the phone is located over there somewhere by that tower; is that basically what you're saying?

A Yes.

Q And is there a radius area for where that phone is located over there by that tower?

A It's oriented to the southwest.

Q Toward the Solar Street over there?

A I can't see the street names.

Q Well, would you look? You have it in front of you there. Isn't this Solar Street that it's oriented toward? And isn't [115] that some other street, northwest, right there that it's oriented towards, that area and Southern Boulevard; isn't that where it's oriented toward?

A Yes.

Q Okay. And did you map that? Did you obtain maps for this particular area?

A That is a map.

Q Okay. You were able to get the basic information to map it, what you call mapping?

A Yes.

Q Okay. And based on that, you concluded that 8507 was right basically in that area where that red dot is, right?

A Yes.

Q Okay. And that's at 2:52 p.m., right?

A The --

Q Well, it says at the top "2:52," right?

A That's the report of the robbery.

Q Pardon me? I'm just saying at 2:52 is where he's supposed to be there, around that red dot, right, where the phone is, right?

A The call at 2:20 puts him on that tower.

Q But the call is 31 minutes, so it goes up to about 2:52, doesn't it?

A Yes.

Q So you're saying he's over there by that red dot at about [116] 2:52, right?

A I'm saying he --

Q The phone is, the phone is, at least?

A Can I answer?

Q Yes.

A I'm saying he utilized that tower for that call.

Q You're saying whoever used that phone utilized that tower, right?

A Yes.

Q Okay. And looking at another one of your maps here for March 4th at 2:52, and this is for the phone number 6845, which has been attributed to Mr. Carpenter; do you see that one?

A Yes.

Q Okay. And this is the map for him, for his phone for 2:52; is that correct?

A Yes.

Q For his alleged phone. And you're saying that he -- that phone was down there by Market Street?

A It used the tower down by Market Street.

Q Okay. That is the tower down at Market Street.

So that means that's a different tower than the other tower you were referring to on the other map, isn't it?

A Entirely different company.

Q Okay, it's a different tower; is that correct?

[117]

A Entirely different company.

Q And the top -- so the answer to my question is, "Yes, it is a different tower, because it's a different company;" isn't that correct?

A Yes.

Q And that tower location is different than the location on the other map, isn't it?

A Yes.

Q And does that indicate that the user of that phone was in a different location?

A No.

Q Why not?

A It's two different companies.

Q But there's two different tower locations?

A Yes. So T-Mobile has a tower in one location and Sprint has a tower in another location.

Q Do the tower locations overlap or do you know?

A It's two different companies, two different technologies, so they would not overlap. They don't communicate with one another.

Q They do not communicate with one another?

A No.

Q So in that regard there is the possibility, based on these two maps, that the person using each of those two phones were in different locations at 2:52?

[118]

A It's apples and oranges.

Q What you mean by that?

A You're talking about one phone that's using the Sprint network, another phone using the T-Mobile network.

Q So you can't really say on the basis of the phone technology if they were or were not in different locations?

A No, I can't. I can only tell you what orientation for each company.

MR. EARLY: Okay, nothing further.

THE COURT: Redirect?

MR. CHADWELL: Can we have Exhibit 57? Put December 13th up. You know what, I can just use that.

REDIRECT EXAMINATION

BY MR. CHADWELL:

Q Agent, can you see your report up there?

A Yes.

Q And I will also be talking about this a little bit, too.

So December 13, 2010, the two towers we are talking about are 127; is that correct?

A Yes.

Q And 145?

A Yes.

Q And 145 being a little closer to the RadioShack than 127, but maybe not by much?

A Right.

[119]

Q And then, just so it's clear to the jury in case the jury can't see, this is tower 145, right?

A Yes.

Q The RadioShack?

A Yes.

Q Now, Agent, can you see -- can you see Defendant's Exhibit 3 there?

A Yes.

Q And do you see up where it says "145"?

A Yes.

Q And do you see the rest of the day?

You see 1:45 up here, in the morning, right?

A Right.

Q Around the time of the robbery?

A Yes.

Q 10:31? So 10:31 we are looking at tower 145, right?

A Right.

Q And then we've got all kinds of other times throughout the day. It's hard to see all this at once, but we've got 11:00, 12:00. We've got 1:00 in the afternoon. All military time here?

A Yes.

Q We've got all the way to 3:24 p.m. on this document, right?

A Correct.

[120]

Q And so the only time that phone is on tower 145 is right around the time of the robbery?

A Correct.

Q According to defendant's own exhibit?

A Correct.

Q Now, we want to talk about the April 5th one for just a second here. I think it was my mistake before when I was pointing up towards Hamtramck. But we can see Hamtramck on this map, can't we?

A Yes.

Q So Hamtramck is kind of at the bottom of the map there.

And then you were asked about some times, too. Let's just make sure the times are clear, in terms of the calls first of all.

Mr. Gurewitz was saying like to 2:30, 2:36. But if we really add up the times, we're talking

about 2:37, aren't we, if we add up 14:21 43 seconds, we get -- plus 15 minutes, 23?

A Yes.

Q That gets us to 2:37, right?

A Yes.

Q And if we assume that the police were not called until 2:40, that's a three-minute difference?

A Yes.

Q Okay. And we don't know all the circumstances of how the [121] police were called. We don't know if people were on the floor, if they had to find their phone or whatever else could have transpired in those three minutes.

But here's what we do know, and correct me if I'm wrong, Agent, that phone was in this sector starting, and it headed into this direction, right?

A Yes.

Q And this is about how far away?

A I believe it is -- the distance between the towers was three-quarters of a mile or so.

Q Okay. So hypothetically, we don't know what direction someone is traveling exactly, but they could have gone up this road and got on McNichols. And by the end of the call, it could have been right here on McNichols, according to the chart; is that right?

A Yes.

Q And if they are heading down McNichols, pretty soon they would be in a position to take a -- first of all they're already on the other side of 75. And

just for the record, they're now on the same side of 75 as Hamtramck, are they not, --

A Right.

Q -- in my hypothetical here?

A Yes.

Q So they might be heading down McNichols and they might be [122] getting ready to take a right-hand turn on Klinger or Charest or McDougall or any number of streets where they could head to Hamtramck?

A Yes, possibly.

Q According to this?

A Yes.

Q Now, they weren't heading back towards the East Jefferson area that we were just looking at, right?

A No, not based on that.

Q They weren't heading in that direction?

A Not based on that, no.

Q So they weren't heading, say, as a crows flies, to Hamtramck, but they were not heading away from Hamtramck?

A Correct.

Q According to your map maker, okay.

MR. CHADWELL: That's all I have, Your Honor.

THE COURT: Mr. Gurewitz?

RECROSS-EXAMINATION

BY MR. GUREWITZ:

Q Agent Hess, I put up on this ELMO projector the map for December 13th.

You indicated a robbery time of 10:35 a.m.; do you see that?

A Yes.

Q And I'll show you again, the Exhibit Three, which is the [123] detail page for this phone number (313) 412-6845 for December 13th, that includes this time.

Mr. Chadwell just asked you questions about the location at the beginning time, the first call that's shown there for that morning.

A Yes.

Q And that is at 10:24?

A Right.

Q And that's the one you said was a tower? What number, please?

A That was on tower 145.

Q And the next one is at 10:31 for --

A I'm sorry, excuse me. You said the 10:24 call?

Q Yes.

A Tower 127.

Q All right. And the next one is at 10:31, at which tower?

A That's on 145. They originated on 145.

Q Now, as I asked you before, following those two calls there are two additional call waiting calls?

A Yes.

Q And what times are those?

A At 10:36 and 10:37.

Q Putting those all together that indicates there is movement at least as to the towers that were used during that time period; isn't that right?

[124]

A From 10:31 to 10:37, yes.

Q In what direction, please?

A To the north, towards 94.

Q According to the duration periods that are on the call detail record, it encompasses the time period that is shown there for the robberies; isn't that right?

A The call waiting calls happen after the reported time of the robbery.

Q So that during the time period of those calls, that's when the reported time of the robbery is on your map, right?

A Yes.

Q Mr. Chadwell asked you questions about whether or not there are any other calls by that number recorded on that report on that day for those same towers; isn't that right?

A Correct.

Q But wouldn't it be relevant to your investigation to be thorough about this, to look at whether or not there was usage by that tell phone of those towers on other days, before or after this, right?

A I would disagree with that.

Q Well, wouldn't that show whether or not the person frequented the particular area that you were looking at for the specific day of December 13, 2010?

A It might.

Q And it would be relevant, wouldn't it, to a total [125] consideration of what the significance of this is to consider whether or not the person had other reasons for being in that neighborhood, right?

A It's a question that may be asked, yes.

Q Such as visiting the relatives of his children, right?

A Possibly.

Q Now, as to April 5, 2011, you were asked questions by Mr. Chadwell just a couple of minutes ago about whether certain routes were possible ways to get to Hamtramck by going north while Hamtramck is south.

Was it part of your investigation to put together this map to take those things into consideration?

A No. Escape routes were not a consideration for me.

Q In fact, you don't even know at the present time whether or not any of -- going north on Woodward, for example, which is about a mile north of the Davison Expressway to McNichols and then traveling over McNichols past all the stores and shops that are along there and the stoplights, was a route that's even feasible as a

way to get directly to Hamtramck that's down here in the lower right-hand corner, right?

A It's certainly feasible.

Q I suppose one could walk there, too. That's feasible as well, right?

A Sure.

MR. GUREWITZ: That's all I have, Your Honor.

* * * * *

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

-v-

Case No.
12-20218

TIMOTHY IVORY CARPENTER and
TIMOTHY MICHAEL SANDERS,

Defendants.

JURY TRIAL – VOLUME EIGHT
BEFORE HON. SEAN F. COX
United States District Judge
257 U.S. Courthouse
231 West Lafayette Boulevard
Detroit, Michigan 48226

(Monday, December 16, 2013)

APPEARANCES:

KENNETH R. CHADWELL, ESQUIRE
Appearing on behalf of the
Government.

HAROLD Z. GUREWITZ, ESQUIRE
JASON EGGERT, ESQUIRE
Appearing on behalf of the
Defendant Timothy Ivory
Carpenter.

S. ALLEN EARLY, ESQUIRE
Appearing on behalf of Defendant
Timothy Michael Sanders.

* * * * *

[55] But he's got three phones and one of them is that number.

Additionally, Little Tim engages in witness tampering in this case. He decides he's going to write up a nice affidavit for Sedric Bell-Gill to sign. And the affidavit just says that Little Tim is innocent of everything. He didn't do nothing, especially with a firearm, according to Sedric Bell-Gill's affidavit that Little Tim provided.

And when you're deliberating, go back and check the date of that affidavit. It's the day before Sedric Bell-Gill is pleading guilty, so there is some urgency in getting that affidavit signed, isn't there, ladies and gentlemen. These prisoners are dumb enough to think that a jury is going to look at an affidavit saying "Little Tim is innocent," and that's it, that's all you've got to think about. These are the actions, ladies and gentlemen, of a guilty person creating false evidence to present to a jury.

I have already mentioned the videos from Ohio as corroboration of what the witnesses are saying. You know they are at Little Caesars, you know what they were doing and you know what time they were at Little Caesars. You know they were at Family Dollar, first of all, buying the bags ahead of that, just like the witnesses said.

Then there's another overlay of corroboration and that is the phone data tracking. Little Tim's phone just [56] happened to be right where the first robbery was at the exact time of the robbery, the exact sector. And that's the only time that entire day,

according to the defense exhibit, he's there. Same thing with December 18, 2010, Little Tim's phone.

March 4, 2011 -- that's kind of unnecessary, right, because they're on video. You know where they're at. But it's also a pretty good check on the phone track data that you know where they're at, but the phone track data tracked that also.

And April 5, 2011, Little Tim's phone right in the right sector before the RadioShack in Highland Park, and shortly afterwards heading not directly to Hamtramck, but in the general direction of Hamtramck. He's not going back to visit the kids back East Jefferson, right? He's heading in the general direction of exactly where our witnesses said he headed, including Hassan.

* * * * *

[63]

* * * * *

And think about that, please, when you go back and you start reviewing what the testimony was of Agent Hess, Agent Hess, the government -- the FBI expert who has this [64] special ability to analyze cell phone tower records and cell tower records, who reached this conclusion. He said it's not an exact science, but it's just his opinion, reached this conclusion that he placed a phone in a particular neighborhood at a certain time. Keep in mind as well, certainly, that all he was able to talk about is that the phone that placed that call was there. He didn't tell you and he acknowledged he can't tell you who actually was using the phone at the time the call was made.

But according to the testimony of these witnesses who lived in those neighborhoods, people who say that they have known Timothy Carpenter all his life, he had every reason in the world to be present on Jefferson Avenue in that neighborhood on December 18 -- excuse me, December 13, 2010, and on Gratiot on December 18, 2010. So that all those records really tell you is that if, in fact, he did have the phone on that day, he was where he lived and spent all of his time. And that's all it says.

* * * * *

[107]

This thing with the towers? You heard testimony from Special Agent Hess that certain phones only communicate with certain types of towers, and that's the reason for these two different maps showing different locations. If you've got a T-Mobile phone, that's only talking to a T-Mobile tower. If you have a Metro PCS phone, it only talks to a Metro PCS tower.

So these two defendants had different types of phones. You know where they were. You saw them on video. There's no question about where these guys were. But Hess's charting of them was different because one phone's talking to this tower and the other phone's talking to this tower.

Also, you saw Mr. Sanders was the only one actually on the phone right at the time of the robbery. And his particular type of phone happened to be -- happened to communicate with the tower that just happened to be closest, right at the robbery scene.

The other call is by Carpenter's phone. You didn't see him on the phone during the robbery. He was making calls before and after and he was probably away from the scene. Or if he wasn't away from the scene, that tower was the -- that type of tower which talks to his type of phone was the closest one and that's why it appears to show him a mile away, but that's really where the tower is.

* * * * *

metroPCS

Call Detail

Records for Target Number: 3134249573

DEFENDANT'S EXHIBIT

CASE NO.

EXHIBIT NO. 7

Search Number: 3134249573 Search Dates: 12/1/2010 - 5/10/2011

12/13/2010	00:04:58	0:36	Outgoing Call	3136294261	3136294261	Answered	None			Detroit1	2	117		2	117
12/13/2010	00:05:38	0:35	Outgoing Call	3136294261	3136294261	Answered	None			Detroit1	1	418		1	418
12/13/2010	00:07:28	0:35	Outgoing Call	3134126406	3134126406	Answered	None			Detroit1	1	418		1	418
12/13/2010	00:08:06	0:34	Outgoing Call	3137782032	3137782032	Answered	None			Detroit1	1	418		1	418
12/13/2010	00:11:09	0:33	Outgoing Call	3137782032	3137782032	Answered	None			Detroit1	1	418		2	117
12/13/2010	00:14:27	0:34	Outgoing Call	3137782032	3137782032	Answered	None			Detroit1	2	117		2	117
12/13/2010	00:15:14	10:32	Incoming Call		3134249573	Answered	None	3134126845	Detroit1	2	117		1	489	
12/13/2010	00:51:26	7:50	Outgoing Call	3134126845	3134126845	Answered	None			Detroit1	5	133		2	117
12/13/2010	00:39:30	0:44	Outgoing Call	4832376	3134832376	Answered	None			Detroit1	3	117		3	117
12/13/2010	00:41:51	1:34	Incoming Call		3134249573	Answered	None	3134126845	Detroit1	2	495		3	461	
12/13/2010	01:02:56	14:09	Incoming Call		3134249573	Answered	None	3132089979	Detroit1	2	117		2	489	
12/13/2010	01:08:58	0:55	Incoming Call		3134249573	Answered	Call Waiting	3134126845	Detroit1	3	117		3	117	
12/13/2010	01:30:06	1:50	Incoming Call		3134249573	Answered	None	3134126845	Detroit1	1	497		2	497	
12/13/2010	08:31:20	0:24	Incoming Call		3134249573	Answered		7344749661	Detroit1	3	111		3	111	
12/13/2010	08:50:20	9:34	Outgoing Call	3134126845	3134126845	Answered	None			Detroit1	1	418		1	418
12/13/2010	09:19:48	1:33	Incoming Call		3134249573	Answered	None	3138781501	Detroit1	1	418		1	418	
12/13/2010	09:32:59	0:27	Outgoing Call	3135754953	3135754953	Answered				Detroit1	3	117		3	117
12/13/2010	09:33:31	3:48	Outgoing Call	3136754399	3136754399	Answered	None			Detroit1	3	117		3	131
12/13/2010	09:38:23	0:42	Outgoing Call	3138781501	3138781501	Answered	None			Detroit1	3	461		3	461
12/13/2010	09:38:22	0:54	Outgoing Call	3716043	3133716043	Answered				Detroit1	3	461		3	131
12/13/2010	09:40:24	1:22	Outgoing Call	3134126845	3134126845	Answered	None			Detroit1	3	131		3	131
12/13/2010	09:45:12	0:37	Outgoing Call	3134126406	3134126406	Answered	None			Detroit1	3	461		2	131
12/13/2010	09:48:04	0:24	Outgoing Call	3134126845	3134126845	Answered	None			Detroit1	3	461		3	461
12/13/2010	09:48:39	0:02	Incoming Call	71313342495	3134249573	Answered	Call FWD - Busy	3134126406	Detroit1						
12/13/2010	09:48:33	0:33	Outgoing Call	3716043	3133716043	Answered				Detroit1	2	131		3	461
12/13/2010	09:59:49	0:05	Outgoing Call	3134126845	3134126845	Answered	None			Detroit1	3	151		3	151
12/13/2010	09:59:58	0:06	Outgoing Call	3134126845	3134126845	Answered	None			Detroit1	2	156		2	156
12/13/2010	10:00:38	0:05	Outgoing Call	3134126845	3134126845	Answered	None			Detroit1	3	151		3	151
12/13/2010	10:00:37	0:04	Incoming Call	71313342495	3134249573	Answered	Call FWD - Busy	3134126845	Detroit1						
12/13/2010	10:09:57	0:26	Incoming Call		3134249573	Answered	None	3134126845	Detroit1	3	131		3	151	
12/13/2010	10:13:17	0:17	Incoming Call		3134249573	Answered	None	3134126845	Detroit1	5	148		5	148	
12/13/2010	10:24:42	5:59	Outgoing Call	3134126845	3134126845	Answered	None			Detroit1	3	146		2	127
12/13/2010	10:31:21	8:23	Incoming Call		3134249573	Answered	None	3134126845	Detroit1	5	164		1	164	
12/13/2010	10:48:54	0:42	Incoming Call		3134249573	Answered		3135201613	Detroit1	5	401		5	401	
12/13/2010	10:50:21	0:26	Outgoing Call	5867440281	5867440281	Answered				Detroit1	5	401		5	401
12/13/2010	10:53:23	0:36	Outgoing Call	2487220120	2487220120	Answered				Detroit1	1	445		1	445
12/13/2010	10:54:49	1:22	Outgoing Call	3135201613	3135201613	Answered				Detroit1	3	164		5	164
12/13/2010	10:56:22	0:32	Outgoing Call	5867440231	5867440281	Answered				Detroit1	5	164		5	164
12/13/2010	11:05:21	0:31	Outgoing Call	7344442530	7344442530	Answered	Outside Home Switch			Detroit2					
12/13/2010	11:05:26	0:27	Incoming Call		3134249573	Answered	Outside Home Switch	2487220120	Detroit1	1	146		1	146	
12/13/2010	11:06:58	0:37	Outgoing Call	3137282481	3137282481	Answered	None			Detroit1	1	146		1	146

metroPCS

DEFENDANT'S EXHIBIT
CASE NO.
EXHIBIT NO. 3

Records for Target Number: 3134126845

Search Number: 3134126845 Search Dates: 12/1/2010 - 3/10/2011

12/13/2010	10:24:47	3:56	Incoming Call		3134126845	Answered	None	3134249573	Detroit1	1	127		2	127
12/13/2010	10:31:18	5:25	Outgoing Call	3134249573	3134249573	Answered	None		Detroit1	3	145		1	164
12/13/2010	10:36:06	0:31	Incoming Call		3134126845	Answered	Call Waiting	3139788284	Detroit1	5	469		3	164
12/13/2010	10:37:21	0:26	Incoming Call		3134126845	Answered	Call Waiting	3139482796	Detroit1	3	164		3	164
12/13/2010	10:42:44	0:50	Incoming Call		3134126845	Answered	None	3139482796	Detroit1	3	164		3	164
12/13/2010	10:52:13	0:09	Incoming Call	7113134126845	3134126845	Answered	Call FWD - No Reply	7015098596	Detroit1	1	445		1	445
12/13/2010	11:31:48	1:19	Incoming Call		3134126845	Answered	None	3137421449	Detroit1	1	418		1	418
12/13/2010	11:45:19	0:36	Incoming Call		3134126845	Answered		5862481054	Detroit1	2	117		2	117
12/13/2010	12:37:33	25:38	Incoming Call		3134126845	Answered	None	3139788284	Detroit1	3	538		1	536
12/13/2010	12:38:27	0:48	Incoming Call		3134126845	Answered	Call Waiting	3134249573	Detroit1	1	538		3	536
12/13/2010	12:44:04	0:00	Outgoing Call	7113134126845	3134126845	Answered	Call Waiting		Detroit1	3	538		3	538
12/13/2010	12:45:25	0:05	Outgoing Call	7113134126845	3134126845	Answered	Call Waiting		Detroit1	3	538		3	538
12/13/2010	13:03:26	5:07	Outgoing Call	3137421449	3137421449	Answered	None		Detroit1	3	538		3	538
12/13/2010	13:04:56	0:24	Incoming Call		3134126845	Answered	Call Waiting	3134249573	Detroit1	3	538		3	538
12/13/2010	13:06:31	1:19	Incoming Call		3134126845	Answered	Call Waiting	5862481054	Detroit1	1	538		3	538
12/13/2010	13:13:42	0:17	Incoming Call		3134126845	Answered	None	3134249573	Detroit1	3	538		3	538
12/13/2010	13:20:15	0:04	Incoming Call	7113134126845	3134126845	Answered	Call FWD - No Reply	3139326811	Detroit2					
12/13/2010	13:20:27	0:46	Outgoing Call	3139326811	3139326811	Answered			Detroit1	6	259		1	259
12/13/2010	13:24:20	9:43	Outgoing Call	7344442427	7344442427	Answered	Outside Home Switch		Detroit2					
12/13/2010	13:24:28	1:39	Incoming Call		3134126845	Answered	Outside Home Switch	3139326811	Detroit1	6	192		6	197
12/13/2010	14:00:35	0:31	Outgoing Call	5862481054	5862481054	Answered			Detroit1	2	401		4	401
12/13/2010	14:00:49	0:57	Outgoing Call	5862481054	5862481054	Answered			Detroit1	2	401		5	401
12/13/2010	14:13:29	2:36	Outgoing Call	3137427201	3137427201	Answered	None		Detroit1	2	382		2	382
12/13/2010	14:15:18	4:26	Outgoing Call	3137783320	3137783320	Answered	None		Detroit1	5	382		3	217
12/13/2010	14:34:10	0:50	Incoming Call		3134126845	Answered	None	3134249573	Detroit1	2	261		1	214
12/13/2010	14:35:15	0:16	Incoming Call		3134126845	Answered	Call Waiting	3137427201	Detroit1	2	261		2	261
12/13/2010	14:56:15	1:14	Outgoing Call	7344442154	7344442154	Answered	Outside Home Switch		Detroit2					
12/13/2010	14:56:29	1:04	Incoming Call		3134126845	Answered	Outside Home Switch	3139326811	Detroit1	3	465		3	465
12/13/2010	15:10:17	0:57	Incoming Call	7113134126845	3134126845	Answered	Call FWD - No Reply	8535135240	Detroit1	3	465		3	465
12/13/2010	15:10:43	0:35	Outgoing Call	3137531168	3137531168	Answered	None		Detroit1	3	465		1	465
12/13/2010	15:15:36	0:42	Outgoing Call	3137531168	3137531168	Answered	None		Detroit1	2	465		2	465
12/13/2010	15:16:23	2:25	Outgoing Call	3134126845	3134126845	Answered	None		Detroit1	2	465		2	465
12/13/2010	15:16:25	0:24	Incoming Call	7113134126845	3134126845	Answered	Call FWD - Busy	3134126845	Detroit1					
12/13/2010	15:17:02	10:58	Outgoing Call	3137531168	3137531168	Answered	None		Detroit1	2	465		2	465
12/13/2010	15:17:15	0:04	Incoming Call	7113134126845	3134126845	Answered	Call FWD - Busy	3139326811	Detroit2					
12/13/2010	15:17:46	0:53	Outgoing Call	7344442454	7344442454	Answered	Outside Home Switch		Detroit2					
12/13/2010	15:17:51	0:50	Incoming Call		3134126845	Answered	Outside Home Switch	3139326811	Detroit1	2	466		2	465
12/13/2010	15:18:46	1:01	Outgoing Call	3137531168	3137531168	Answered	None		Detroit1	2	465		1	186
12/13/2010	15:21:23	0:59	Outgoing Call	7344442357	7344442357	Answered	Outside Home Switch		Detroit2					
12/13/2010	15:21:26	0:57	Incoming Call		3134126845	Answered	Outside Home Switch	3139326811	Detroit1	3	465		3	465
12/13/2010	15:24:39	13:28	Outgoing Call	5862481054	5862481054	Answered			Detroit1	1	188		2	465

RECORD AND BRIEFS

No. 16-402

FILED
AUG - 7 2017
OFFICE OF THE CLERK
SUPREME COURT, U.S.

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

—v.—

UNITED STATES OF AMERICA,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

BRIEF FOR PETITIONER

Nathan Freed Wessler
Ben Wizner
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004

David D. Cole
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
915 15th Street, NW
Washington, DC 20005

Cecillia D. Wang
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111

Harold Gurewitz
Counsel of Record
GUREWITZ & RABEN, PLC
333 W. Fort Street, Suite 1400
Detroit, MI 48226
(313) 628-4733
hgurewitz@grplc.com

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
AMERICAN CIVIL LIBERTIES UNION FUND OF MICHIGAN
2966 Woodward Ave.
Detroit, MI 48201

Jeffrey L. Fisher
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305

QUESTION PRESENTED

Whether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 127 days is permitted by the Fourth Amendment.

PARTIES TO THE PROCEEDINGS

In addition to the parties named in the caption, Timothy Michael Sanders was a defendant appellant below, and was represented by separate counsel.

TABLE OF CONTENTS

QUESTION PRESENTED i

PARTIES TO THE PROCEEDINGS ii

TABLE OF AUTHORITIES xiii

BRIEF FOR PETITIONER 1

OPINIONS BELOW 1

JURISDICTION 1

RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS 1

STATEMENT OF THE CASE 3

SUMMARY OF ARGUMENT 10

ARGUMENT 14

I. THE ACQUISITION OF LONGER-TERM CELL SITE LOCATION INFORMATION CONSTITUTES A SEARCH 14

A. Individuals Have A Reasonable Expectation Of Privacy In Their Longer-Term Cell Phone Location Records 14

B. Law Enforcement Access To Cell Site Location Information Interferes With The Security Of A Person's Private "Papers." 32

C. Pre-Digital Cases Concerning The Third-Party Doctrine Do Not Govern This Case 35

1. Cell Site Location Information is Far More Sensitive than the Phone and Bank Records Involved in *Smith* And *Miller*, and Unlike Those Records, is Not Voluntarily Conveyed 35

2. Extending *Smith* and *Miller* to CSLI Records Would Remove a Great Volume of Other Similarly Sensitive Digital Records from the Protection of The Fourth Amendment 44

II. SEARCHING CELL SITE LOCATION INFORMATION IS UNREASONABLE WITHOUT A WARRANT 47

A. Congress Has Not Had An Opportunity To Consider This Problem 49

B. Analogy To This Court's Subpoena Cases Does Not Render The Search Reasonable 51

C. A Balancing Of Interests Under The Fourth Amendment Commands That A Warrant Is Required 53

CONCLUSION 58

TABLE OF AUTHORITIES

CASES

Arizona v. Gant, 556 U.S. 332 (2009) 49

Baldwin v. New York, 399 U.S. 66 (1970) 30

California v. Ciraolo, 476 U.S. 207 (1986) 22

Camara v. Municipal Ct., 387 U.S. 523 (1967) 54

City of L.A. v. Patel, 135 S. Ct. 2443 (2015) 49

City of Ontario v. Quon, 560 U.S. 746 (2010) 40, 29

Commonwealth v. Augustine,
4 N.E.3d 846 (Mass. 2014) 17, 19, 22, 30

Commonwealth v. Estabrook,
38 N.E.3d 231 (Mass. 2015) 31

Coolidge v. New Hampshire, 403 U.S. 443 (1971) ... 54

Couch v. United States,
409 U.S. 322 (1973) 51, 52, 53

Cty. of Riverside v. McLaughlin,
500 U.S. 44 (1991) 30

Cutter v. Wilkinson, 544 U.S. 709 (2005) 48

Donovan v. Lone Steer, Inc., 464 U.S. 408 (1984) 53

Ferguson v. City of Charleston, 532 U.S. 67 (2001). 37

Florida v. Jardines, 133 S. Ct. 1409 (2013) 32, 33

Florida v. Riley, 488 U.S. 445 (1989) 21, 38

Ford v. State,
477 S.W.3d 321 (Tex. Crim. App. 2015) 31

In re Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011 (N.D. Cal. 2015) 43

In re Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526 (D. Md. 2011) 29

In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) 25

Johnson v. United States, 333 U.S. 10 (1948) 52

Kastigar v. United States, 406 U.S. 441 (1972) 19

Katz v. United States, 389 U.S. 347 (1967) .....*passim*

Kyllo v. United States, 533 U.S. 27 (2001) .....*passim*

Maryland v. King, 133 S. Ct. 1958 (2013) 54

Maryland v. Shatzer, 559 U.S. 98 (2010) 30

Minnesota v. Olson, 495 U.S. 91 (1990) 15

Okla. Press Publ'g Co. v. Walling, 327 U.S. 186 (1946) 51

People v. Blair, 602 P.2d 738 (Cal. 1979) 44

S.E.C. v. Jerry T. O'Brien, Inc., 467 U.S. 735 (1984) 53

Riley v. California, 134 S. Ct. 2473 (2014) .....*passim*

Smith v. Maryland, 442 U.S. 735 (1979) .....*passim*

Stanford v. Texas, 379 U.S. 476 (1965) 57

State v. Earls, 70 A.3d 630 (N.J. 2013) 17, 23

State v. Walton, 324 P.3d 876 (Haw. 2014) 44

Stoner v. California, 376 U.S. 483 (1964) 37

Tennessee v. Garner, 471 U.S. 1 (1985) 21

Terry v. Ohio, 392 U.S. 1 (1968) 30

Tracey v. State, 152 So. 3d 504 (Fla. 2014) 23, 31

United States v. Davis,
785 F.3d 498 (11th Cir. 2015) ..... *passim*

United States v. Davis,
754 F.3d 1205 (11th Cir. 2014) 17

United States v. Espudo,
954 F. Supp. 2d 1029 (S.D. Cal. 2013) 55

United States v. Graham,
824 F.3d 421 (4th Cir. 2016) ..... *passim*

United States v. Graham,
846 F. Supp. 2d 384 (D. Md. 2012) 25

United States v. Hubbell, 530 U.S. 27 (2000) 53

United States v. Jones, 565 U.S. 400 (2012) ..... *passim*

United States v. Karo, 468 U.S. 705 (1984) 18

United States v. Knotts, 460 U.S. 276 (1983) 20, 37

United States v. Miller, 425 U.S. 435 (1976) ..... *passim*

United States v. Morton Salt Co.,
338 U.S. 632 (1950) 51

United States v. Pineda-Moreno,
617 F.3d 1120 (9th Cir. 2010) 21

United States v. Place, 462 U.S. 696 (1983) 30

United States v. Powell, 379 U.S. 48 (1964) 51

United States v. R. Enterprises, Inc.,
498 U.S. 292 (1991) 53

United States v. Riley,
858 F.3d 1012 (6th Cir. 2017) 31

United States v. Robinson, 414 U.S. 218 (1973) 54

United States v. Skinner,
690 F.3d 772 (6th Cir. 2012) 31

United States v. Sparks,
711 F.3d 58 (1st Cir. 2013) 20

United States v. Stimler, __ F.3d __,
2017 WL 3080866 (3d Cir. July 7, 2017) 26, 57

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 46

United States v. Watson, 423 U.S. 411 (1976) 21

U.S. West, Inc. v. F.C.C.,
182 F.3d 1224 (10th Cir. 1999) 34

United States v. Wigginton,
No. 6:15-CR-5-GFVT-HAI-1,
2015 WL 8492457 (E.D. Ky. Dec. 10, 2015) 31

United States v. Williams,
161 F. Supp. 3d. 846 (N.D. Cal. 2016) 57

CONSTITUTION & STATUTES

U.S. Const. amend. IV ..... *passim*

18 U.S.C. § 924(c) 9

Hobbs Act, 18 U.S.C. § 1951(a) 9

Stored Communications Act,
18 U.S.C. § 2703 ..... *passim*

18 U.S.C. § 2703(c)(1)(A) 50

18 U.S.C. § 2703(c)(3) 52

18 U.S.C. § 2703(d) ..... *passim*

28 U.S.C. § 1254(1) 1

47 U.S.C. § 207 33

47 U.S.C. § 222 ..... *passim*

49 U.S.C. § 40103 22

Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) .. 50

Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286 33

12 R.I. Gen. Laws § 12-32-2 22

725 Ill. Comp. Stat. 168/10 23

Cal. Penal Code § 1546.1 22

Ind. Code § 35-33-5-12 23

Kan. Stat. Ann. § 22-2502 22

Md. Code Ann. Crim. Proc. § 1-203.1 23

Me. Rev. Stat. tit. 16, § 648 22

Minn. Stat. § 626A.28 22

Minn. Stat. § 626A.42 22

Mont. Code Ann. § 46-5-110 22

N.H. Rev. Stat. Ann. § 644-A:2 22

Utah Code Ann. § 77-23c-102 22

Vt. Stat. Ann. tit. 13, § 8102 22

LEGISLATIVE MATERIALS

145 Cong. Rec. H9858 01 (daily ed. Oct. 12, 1999) (statement of Rep. Tauzin) 22

H.R. Rep. No. 103-827 (1994) 50

H.R. Rep. No. 99-647 (1986) 50

Letter from Aaron Maguire, Legislative Counsel, Cal. State Sheriff's Ass'n, to Sen. Mark Leno, Cal. State Senate (Aug. 26, 2015) 55

Letter from Charles McKee, Vice President, Sprint Nextel, to Sen. Edward J. Markey (Oct. 3, 2013) 20

Letter from David Bejarano, President, Cal. Police Chiefs Ass'n, Inc., to Hon. Mark Leno, Cal. State Senate (Aug. 24, 2015) 55

Letter from Timothy P. McKone, Executive Vice President, AT&T, to Sen. Edward J. Markey (Oct. 3, 2013) 20

Letter from William B. Petersen, Gen. Counsel, Verizon Wireless, to Sen. Edward J. Markey (Oct. 3, 2013) 20

S. Rep. No. 99-541 (1986) 50

The Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism & Homeland Sec. of the H. Comm. on the Judiciary, 113th Cong. 15 (2013) (statement of Matt Blaze, Assoc. Professor, Univ. of Pa.) 27

OTHER AUTHORITIES

Am. Civil Liberties Union, *ACLU Affiliate Nationwide Cell Phone Tracking Public Records Requests: Findings and Analysis* (2013) 55

Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 Cal. L. Rev. 805 (2016) 46

Apple, *iPhone User Guide: Location Services* 42

Cal. Dep't of Justice, Office of the Attorney Gen., *Electronic Search Warrant Notifications* 56

Christopher Slobogin, *Subpoenas and Privacy*, 54 DePaul L. Rev. 805 (2005) 51

Craig Silliman, Exec. Vice President, Pub. Pol'y & Gen. Counsel, Verizon, *Technology and Shifting Privacy Expectations*, Bloomberg Law, Oct. 7, 2016 ..... 4, 20, 27, 28

CTIA, *Annual Wireless Industry Survey* (2017) 4, 28, 50

CTIA, *Background on CTIA's Wireless Industry Survey* (2014) 50

CTIA, *Wireless Snapshot 2017* 28

Eric J. Topol, *The Future of Medicine Is in Your Smartphone*, Wall St. J., Jan. 9, 2015 41

F.C.C., *911 Wireless Services* 41

F.C.C., Indus. Analysis & Tech. Div., *Payphone Data from 1997 Through 2016* (2017) 40

Hendrik Müller et al., *Understanding and Comparing Smartphone and Tablet Use: Insights from a Large-Scale Diary Study*, Proceedings of the 27th Australian Computer-Human Interaction Conference 427 (2015) 17

Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 28 FCC Rcd. 9609 (2013) 33

In re Wireless E911 Location Accuracy Requirements, PS Docket No. 07-114 (F.C.C. Jan. 29, 2015) 28

Joseph Hoy, *Forensic Radio Survey Techniques for Cell Site Analysis* (2015) ..... *passim*

Kashmir Hill, *This Sex Toy Tells the Manufacturer Every Time You Use It*, Fusion, Aug. 9, 2016..... 46

Maxwell Payne, *How to Turn Off GPS on a Cell Phone*, USA Today..... 42

Megha Rajagopalan, *Cellphone Companies Will Share Your Location Data – Just Not With You*, ProPublica, June 26, 2012 43

MetroPCS, Annual 47 C.F.R. § 64.2009(e) CPNI Certification, EB Docket 06-036 (Mar. 1, 2011)... 34

Michael Carroll, *Small Cells Hit Milestone*, FierceWireless, Nov. 1, 2012..... 28

Moira Weigel, *'Fitbit for Your Period': The Rise of Fertility Tracking*, Guardian, Mar. 23, 2016..... 46

Neal Walfield et al., *A Quantitative Analysis of Cell Tower Trace Data for Understanding Human Mobility and Mobile Networks*, 6th International Workshop on Mobile Entity Localization, Tracking and Analysis (Oct. 10, 2016) 26

Pew Research Ctr., *U.S. Smartphone Use in 2015* (2015) 41

Richard M. Re, *The Positive Law Floor*, 129 Harv. L. Rev. F. 313 (2016)..... 32

Rodrigo de Oliveira et al., *Towards a Psychographic User Model from Mobile Phone Usage*, Proceedings of the ACM CHI 2011 Conference on Human Factors in Computing Systems (2011) 26

Second Report & Order and Further Notice of Proposed Rulemaking, *In re Implementation of the Telecommunications Act of 1996*, 13 FCC Rcd. 8061 (1998) 34

Sibren Isaacman et al., *Identifying Important Places in People's Lives from Cellular Network Data*, Proc. of 9th International Conference on Pervasive Computing (June 2011) 26

Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373 (2006) 23

Stephen J. Blumberg & Julian V. Luke, Ctrs. for Disease Control & Prevention, Nat'l Ctr. for Health Statistics, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July–December 2016* (2017) 40

Tim Moynihan, *Alexa and Google Home Record What You Say. But What Happens to that Data?*, Wired, Dec. 5, 2016 46

T-Mobile, *Transparency Report for 2013 & 2014* (2015) 56

William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv. L. Rev. 1821 (2016) 22, 32

BRIEF FOR PETITIONER

Petitioner Timothy Carpenter respectfully requests that this Court reverse the judgment of the United States Court of Appeals for the Sixth Circuit.

OPINIONS BELOW

The opinion of the Sixth Circuit (Pet. App. 1a-32a) is reported at 819 F.3d 880. The district court opinion (Pet. App. 34a-48a) is unpublished, but is available at 2013 WL 6385838.

JURISDICTION

The Sixth Circuit issued its opinion on April 13, 2016, and denied rehearing en banc on June 29, 2016. Pet. App. 33a. This Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS

The Fourth Amendment to the U.S. Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Stored Communications Act, 18 U.S.C. § 2703, provides in relevant part:

(c) Records concerning electronic communication service or remote computing service.--**(1)** A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--

> **(A)** obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; [or]
>
> **(B)** obtains a court order for such disclosure under subsection (d) of this section; * * *

(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. * * *

STATEMENT OF THE CASE

1. This case concerns governmental acquisition of personal location records, known as cell site location information ("CSLI"), to identify Petitioner Timothy Carpenter's whereabouts over more than four months. The records, which are logged and retained by cellular service providers whenever people carry modern cell phones, make it possible to reconstruct in detail everywhere an individual has traveled over hours, days, weeks, or months.

In order to access the cellular network, cell phones must connect to nearby cell towers (known as "cell sites"), thereby creating a record of the phone's location. The precision of a cell phone user's location reflected in CSLI records depends on the size of the cell site "sectors" in the area. Most cell sites consist of multiple directional antennas that divide the cell site into sectors. Pet. App. 5a. The majority of cell sites comprise three directional antennas that divide the cell site into three sectors (usually 120 degrees each), but an increasing number of towers have six antennas (covering approximately 60 degrees each). Pet. App. 14a; *see also* Joseph Hoy, *Forensic Radio Survey Techniques for Cell Site Analysis* 61 (2015). The coverage area of each cell site sector is smaller in areas with greater density of cell sites, with urban areas having the greatest density and thus the smallest coverage areas. Pet. App. 5a; *see also* Pet. App. 87a (Gov't Trial Ex. 57, at 13) (providing maps of MetroPCS and Sprint cell sites). The smaller the coverage area, the more precise the location information revealed and recorded.

The density of cell sites continues to increase as data usage from smartphones grows. Because each

cell site carries a fixed volume of data required for text messages, emails, web browsing, streaming video, and other uses, as smartphone data usage increases, carriers erect additional cell sites, each covering smaller geographic areas. *See* CTIA, *Annual Wireless Industry Survey* 4 (2017)[1] (number of cell sites in the United States increased from 195,613 to 308,334 from 2006 to 2016); *id.* at 3 (annual wireless data usage increased more than 3,500 percent from 2010 to 2016). This means that in urban and dense suburban areas like Detroit, many sectors cover small geographic areas. Pet. App. 5a.

Service providers have long retained location information for the start and end of incoming and outgoing calls. Pet. App. 5a-6a. Today, those companies increasingly also retain location information related to the transmission of text messages and routine internet connections—which smartphones make virtually constantly to check for new emails, social media messages, weather updates, and other functions. *See* Craig Silliman, Exec. Vice President, Pub. Pol'y & Gen. Counsel, Verizon, *Technology and Shifting Privacy Expectations*, Bloomberg Law, Oct. 7, 2016.[2] The information recorded can include not only cell site and sector, but also estimated distance of the phone from the nearest cell site. *Id.* Location precision is also increasing as service providers deploy millions of "small cells," "which cover a very specific area, such as one floor of

---

[1] https://www.ctia.org/docs/default-source/default-document-library/annual-year-end-2016-top-line-survey-results-final.pdf.

[2] https://bol.bna.com/technology-and-shifting-privacy-expectations-perspective.

a building, the waiting room of an office, or a single home." *United States v. Graham*, 824 F.3d 421, 448 (4th Cir. 2016) (en banc) (Wynn, J., dissenting in part and concurring in the judgment) (citation omitted); *see also* Hoy, *supra*, at 69-70.

All told, a typical smartphone connects to cell towers hundreds of times a day, generating a densely pixelated matrix of data points documenting the user's movements. The volume and precision of that data will grow steadily in coming years, generating ever more granular locational information.

Congress has explicitly recognized the sensitivity of CSLI. The Telecommunications Act treats this data as proprietary to the customer, and bars cellular service providers from sharing a customer's CSLI without the customer's express advance approval. 47 U.S.C. § 222(c)(1)-(2), (f).

2. In 2011, officers from the Detroit Police Department arrested four individuals they thought had robbed Radio Shack and T-Mobile stores in Detroit, Michigan. Pet. App. 53a. One of the arrestees "admitted he had a role in eight different robberies that started in December of 2010 and lasted through March of 2011 at Radio Shack and T-Mobile stores in Michigan and Ohio. . . . The [arrestee] identified 15 other individuals who had been involved in at least one of the eight robberies." Pet. App. 53a-54a.

An Assistant United States Attorney then submitted three applications for orders to access 152 days of historical cell phone location records for Timothy Carpenter and several other suspects. Pet. App. 3a, 49a-55a, 62a-68a. The applications, which

were unsworn, did not seek warrants based on probable cause, but rather orders under a 1986 law, the Stored Communications Act ("SCA"), 18 U.S.C. § 2703(d). SCA orders may issue when the government "offers specific and articulable facts showing that there are reasonable grounds to believe that" the records sought "are relevant and material to an ongoing criminal investigation." *Id.*

The primary application at issue here asserted that "the requested records will assist in identifying and locating the other individuals believed to be involved in the armed robberies" and "provide evidence that . . . Timothy Carpenter and other known and unknown individuals are violating provisions of Title 18, United States Code, §1951." Pet. App. 54a. The application sought "[a]ll subscriber information, toll records and call detail records . . . from [the] target telephones from December 1, 2010 to present[,]" as well as "cell site information for the target telephones at call origination and at call termination for incoming and outgoing calls[.]" Pet. App. 4a (some alterations in original); *see also* Pet. App. 52a.

Magistrate judges issued two separate orders granting the applications for Carpenter's records. Pet. App. 56a-61a, 69a-73a. (The third order, also granted, sought CSLI of other suspects). The first order directed MetroPCS, Carpenter's cellular service provider, to "provide the locations of cell/site sector (physical addresses) for the target telephones at call origination and at call termination for incoming and outgoing calls" from "December 1, 2010 to present [May 2, 2011]." Pet. App. 59a-61a. MetroPCS complied, providing 186 pages of Carpenter's cell

phone records (known as "call detail records") to the government.[3] Those records show the cell site and sector that Carpenter's phone connected to at the start and end of most of his incoming and outgoing calls over the course of 127 days.[4] Pet. App. 5a-7a.

The second order directed Sprint to produce cell site location information for Carpenter's phone while it was "roaming on Sprint's cellular tower network" for seven days in March, 2011. Pet. App. 72a. "Metro PCS does not have coverage in the Warren, Ohio area," where one of the charged robberies took place, and has a "roaming agreement . . . with Sprint, which does cover that area." J.A. 63. Therefore, Sprint, not MetroPCS, possessed Carpenter's CSLI for his time spent in and around Warren. Sprint produced two days' worth of CSLI.

MetroPCS and Sprint also produced lists of their cell sites in southern Michigan and northwestern Ohio, respectively, providing the longitude, latitude, and physical address of each cell site, along with the directional orientation of each sector antenna. *See* J.A. 79. Cross-referencing the information in Carpenter's call detail records with

---

[3] Two pages from Carpenter's records were introduced at trial. J.A. 135-36 (Defendant's Trial Exs. 2 & 3). The government provided the full records to the defense in discovery and a prosecution witness discussed them at trial. J.A. 50-51. The full CSLI records were filed as an appendix to the Amicus Brief of the American Civil Liberties Union et al. at the Sixth Circuit. *See* 6th Cir. Doc. No. 33-1.

[4] Although the government's application and resulting court order sought 152 days of records, MetroPCS produced 127 days of records.

these cell site lists allowed law enforcement to identify the area in which Carpenter's phone was located and thereby to deduce Carpenter's location and movements over the course of each day.

All told, the government obtained 12,898 CSLI data points tracing Carpenter's movements—an average of 101 location points per day for more than four months' time. 6th Cir. Doc. No. 29, at 9.

3. Before trial, Carpenter moved to suppress the CSLI records on the basis that the Fourth Amendment prohibits their acquisition without probable cause and a warrant. Pet. App. 36a-37a; *see also id.* at 4a. The district court denied the motion, reasoning that people do not have a reasonable expectation of privacy in CSLI records—and, consequently, their acquisition by the government does not constitute a "search" under the Fourth Amendment. Pet. App. 38a-39a.

At trial, FBI Special Agent Christopher Hess testified that Carpenter's CSLI placed him near four of the charged robberies. Pet. App. 5a-6a. Hess produced maps, constructed using the CSLI, which showed the location of Carpenter's phone relative to the locations of the robberies. Pet. App. 6a; *id.* at 85a-89a (Gov't Trial Ex. 57). The government relied on the records to show Carpenter's proximity to "the robberies around the time the robberies happened." Pet. App. 6a. The prosecutor argued to the jury, for example, that Carpenter was "right where the first robbery was at the exact time of the robbery, the exact sector," J.A. 131, and that he was "right in the right sector before the RadioShack [robbery] in Highland Park," J.A. 132; *see also* J.A. 53-67 (testimony of Special Agent Hess).

The jury convicted Carpenter of six robberies in violation of the Hobbs Act, 18 U.S.C. § 1951(a), and five separate violations of 18 U.S.C. § 924(c) for using or carrying a firearm in connection with a federal crime of violence and aiding and abetting the commission of that offense. The court sentenced Carpenter to nearly 116 years' imprisonment.

4. A divided panel of the Sixth Circuit affirmed. The panel majority acknowledged that in *United States v. Jones*, 565 U.S. 400 (2012), five Justices agreed that people have a reasonable expectation of privacy in information very similar to the CSLI data obtained here –namely, "longer term GPS monitoring in government investigations of most offenses." Pet. App. 13a (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment)). But the majority held that individuals have no reasonable expectation of privacy in cell phone location records. Pet. App. 17a. It distinguished *Jones* on the ground that "[t]his case involves business records obtained from a third-party," Pet. App. 14a, which the majority viewed as more like the landline calling records that this Court held in 1979 were not entitled to Fourth Amendment protection, Pet. App. 11a-12a (citing *Smith v. Maryland*, 442 U.S. 735 (1979)). The majority also noted that the GPS information in *Jones* was "accurate enough to show that the target [was] located within an individual building," while CSLI was less precise. Pet. App. 14a-15a.

Judge Stranch disagreed. Concurring in the judgment only, she explained that "the sheer quantity of sensitive information procured without a warrant in this case raises Fourth Amendment

concerns of the type the Supreme Court . . . acknowledged in [*Jones*]." Pet. App. 24a. "I do not think that treating the CSLI obtained as a 'business record' and applying that test addresses our circuit's stated concern regarding long-term, comprehensive tracking of an individual's location without a warrant." *Id.* at 29a. Judge Stranch concluded, however, that suppression was not warranted under the good-faith exception to the exclusionary rule, a question that the majority did not address. *Id.* at 29a-31a.

SUMMARY OF ARGUMENT

I. Under this Court's recent Fourth Amendment cases, the government conducted a search when it obtained 127 days of petitioner's cell phone location records from his cellular service provider.

A. When the government employs new technology to obtain sensitive personal information in a way that diminishes the degree of privacy that individuals reasonably expected prior to the technology's adoption, it conducts a search under the Fourth Amendment. Applying this principle in *United States v. Jones*, 565 U.S. 400 (2012), five Justices concluded that longer-term GPS tracking of a car violates reasonable expectations of privacy. Tracing a person's geographical movements reveals highly sensitive personal information, and prior to the digital age, people reasonably expected that police in most investigations would not have followed a person and recorded her every movement for days or weeks on end.

The same analysis controls this case. CSLI exposes a great volume of highly sensitive information about a person, revealing where she has been and whom she has been with throughout each day. And as acute as that concern is today, it will only sharpen over time, as the volume and precision of CSLI records steadily increases. Furthermore, just as with GPS tracking, the government prior to the widespread proliferation of cell phones could have obtained only very limited information about a person's past geographical movements. Police officers could have, for example, interviewed witnesses, sought security camera footage, or examined store receipts near the scene of a crime. But these tactics pale in comparison to the unprecedented surveillance time machine that CSLI provides.

In addition, obtaining CSLI records invades an individual's Fourth Amendment right to security in his private "papers." Federal law grants individuals a proprietary interest in their CSLI records by prohibiting service providers from disclosing that information without "express prior authorization of the customer." 47 U.S.C. § 222(f). Wholly apart from a reasonable-expectation-of-privacy analysis, the government's impingement on that interest for purposes of gathering information constitutes a search.

B. Contrary to the Sixth Circuit's view, decades-old cases involving the "third-party doctrine" do not render the Fourth Amendment inapplicable here. In *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), this Court concluded that people lack a reasonable expectation of privacy in dialed telephone numbers

and banking records, because of the records' limited sensitivity and because the information involved was voluntarily conveyed to third parties. But a great gulf divides those cases from the investigative activity at issue here.

The detailed and pervasive location records obtained in this case are far more comprehensive and sensitive than discrete telephonic or banking information. And location data is not "voluntarily" conveyed by a phone user in the same sense as the information in *Smith* and *Miller*. Cell phones are indispensable to participation in modern society—often required for employment, relied on for personal safety, and increasingly becoming essential medical treatment tools. Even if it could be said that *possessing* a cell phone is a voluntary act, it certainly cannot be said that cell phone owners knowingly and intentionally disclose their minute-by-minute movements in historical perpetuity. Carrying a smartphone, checking for new emails from one's boss, updating the weather forecast, and downloading directions ought not license total surveillance of a person's entire life.

As this Court's decisions in *Jones*, 565 U.S. 400, and *Riley v. California*, 134 S. Ct. 2473 (2014), illustrate, the innovations of the digital age preclude wooden extension of analog-era precedents where technology has greatly increased the government's ability to obtain intimate information. Extending *Smith* and *Miller* to CSLI would lead to unacceptable consequences. It would mean not only that CSLI is exempt from the Fourth Amendment, but also that persons would lack any reasonable expectation of privacy in the contents of emails and other

communications that are necessarily shared with service providers to enable their transmission. People reasonably expect that the details of where they travel over an extended period are known only to themselves, and therefore cannot be obtained by the government without implicating the Fourth Amendment.

II. This Court may wish to allow the Sixth Circuit to determine in the first instance whether a search of CSLI pursuant to an order under the Stored Communications Act is "reasonable" under the Fourth Amendment. Should the Court reach the question, however, it should hold that such a search is unreasonable.

The usual rule is that a warrant is required for criminal investigative searches. And Congress has not decreed here to the contrary. Congress enacted the SCA prior to the widespread proliferation of cell phones and without awareness of the coming availability of CSLI.

Nor does any exception to the warrant requirement apply here. The government argues that its subpoena power allows it to obtain CSLI records on a showing of less than probable cause. But the subpoena power allows the government merely to obtain business records in which businesses have a diminished expectation of privacy, if they have any at all. This Court has never extended that power to records as to which individuals have a reasonable expectation of privacy. And allowing warrantless access to such information—particularly CSLI records—would constitute a massive expansion of government power and a threat to personal privacy

akin to the general warrants that the Framers of the Fourth Amendment so abhorred.

ARGUMENT

I. THE ACQUISITION OF LONGER-TERM CELL SITE LOCATION INFORMATION CONSTITUTES A SEARCH.

The Sixth Circuit held—and the government argues—that the Fourth Amendment does not restrict access to CSLI because it involves no "search" or "seizure." If the Court were to accept this argument, the government could use this tool to monitor the minute-by-minute whereabouts of anyone—from ordinary citizens to prominent businesspersons to leaders of social movements. The implication of the government's position is not that it should be able to obtain CSLI about particular suspects in particular investigations pursuant to orders under § 2703(d) of the Stored Communications Act; Congress could repeal that statute tomorrow. Rather, it is that the government could obtain every American's location history detailing their movements 24 hours a day, seven days a week, month after month, with no quantum of suspicion or judicial oversight whatsoever. That sweeping proposition is incompatible with the requirements of the Fourth Amendment.

A. Individuals Have A Reasonable Expectation Of Privacy In Their Longer-Term Cell Phone Location Records.

1. Under this Court's longstanding test, government agents engage in a Fourth Amendment

search when they intrude on an expectation of privacy that society is prepared to recognize as reasonable. *Kyllo v. United States*, 533 U.S. 27, 33 (2001); *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The touchstone for determining when an expectation of privacy is reasonable is "the everyday expectations of privacy that we all share." *Minnesota v. Olson*, 495 U.S. 91, 98 (1990). For example, this Court held in *Katz* that the Fourth Amendment applies to conversations transmitted over telephone lines because phones played a "vital role" in conducting the type of communication previously treated as "private." 389 U.S. at 352-53.

As new technology has dramatically lowered the cost of government surveillance and increased the government's access to private information, this Court has stressed that the reasonable-expectation-of-privacy inquiry must "assur[e] preservation of that degree of privacy against government that existed" prior to the advent of the new technology in question. *United States v. Jones*, 565 U.S. 400, 406 (Scalia, J.) (alteration in original); *id.* at 420 (Alito, J., concurring in the judgment); *Kyllo*, 533 U.S. at 34; *see also Riley v. California*, 134 S. Ct. 2473, 2490 (2014) (requiring a warrant to search contents of cell phones seized incident to arrest in order to preserve degree of privacy enjoyed before invention and pervasive use of cell phones).

Applying this framework in *United States v. Jones*, five Justices agreed that people have a reasonable expectation of privacy in "longer term GPS monitoring in investigations of most offenses." *Jones*, 565 U.S. at 430 (Alito, J., concurring in the

judgment); *id.* at 415 (Sotomayor, J., concurring). Because GPS monitoring of a car tracks "every movement" a person makes in that vehicle, *id.* at 430 (Alito, J., concurring in the judgment), it generates extremely sensitive and private information that "enables the Government to ascertain, more or less at will, [people's] political and religious beliefs, sexual habits, and so on," *id.* at 416 (Sotomayor, J., concurring). Prior to the digital age, this information would have been largely immune from search. Although historically the government could have tasked a team of agents with surreptitiously tailing a suspect, doing so "for any extended period of time was difficult and costly and therefore rarely undertaken." *Id.* at 429 (Alito, J., concurring in the judgment). Therefore, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.* at 430.

2. These principles dictate that government agents conduct a search when they obtain longer-term historical cell phone location records from a person's cellular service provider.

a. For the same reason that five Justices concluded that there is a reasonable expectation of privacy in longer-term GPS monitoring of a car, there is a reasonable expectation of privacy in longer-term cell phone location records. Any other conclusion would allow the government to circumvent the principle accepted by five Justices in *Jones* through the simple expedient of obtaining cell phone location records. People use their cell phones throughout the day—when they are at home, work, or school, when

they are in the car or on public transportation, when they are shopping or eating, and when they are visiting the doctor, a lawyer, a political associate, or a friend.[5] People even keep their phones nearby and turned on while they are asleep.[6] Indeed, "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower." *Riley*, 134 S. Ct. at 2490.

"[D]etails about the location of a cell phone can provide an intimate picture of one's daily life." *State v. Earls*, 70 A.3d 630, 642 (N.J. 2013). Historical CSLI "can reveal not just where people go—which doctors, religious services, and stores they visit—but also the people and groups they choose to affiliate with and when they actually do so." *Commonwealth v. Augustine*, 4 N.E. 3d 846, 861 (Mass. 2014) (quoting *Earls*, 70 A.3d at 642). And to state the obvious, when people make a "visit to a gynecologist, a psychiatrist, a bookie, or a priest," they typically "assume that the visit is private." *United States v. Davis*, 754 F.3d 1205, 1216 (11th Cir. 2014) (Sentelle, J.), *rev'd en banc*, 785 F.3d 498 (11th Cir. 2015).

CSLI can also reveal that people are present in their own homes or the homes of their closest friends and relatives, even when that fact is otherwise undiscoverable. Such information gathering "falls

---

[5] Hendrik Müller et al., *Understanding and Comparing Smartphone and Tablet Use: Insights from a Large-Scale Diary Study*, Proceedings of the 27th Australian Computer-Human Interaction Conference 427, 432 (2015), https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/44200.pdf.

[6] *Id.*

within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance" from a public place, such as whether "a particular article is actually located at a particular time in the private residence," or to later confirm that the article remains on the premises. *United States v. Karo*, 468 U.S. 705, 707, 715 (1984).

b. Allowing law enforcement to obtain such records free and clear of any Fourth Amendment restriction would dramatically shrink the amount of privacy that people enjoyed from the time of the Framing through the dawn of the digital age. Prior to the widespread adoption of cell phones, the government simply could not have obtained a comprehensive record of a person's past locations and movements over an extended period. Even "in the context of investigations involving extraordinary offenses," *Jones*, 565 U.S. at 431 (Alito, J., concurring in the judgment), law enforcement agents could have retrieved at best only fragmentary historical location records: perhaps an employee's timecard from the start of a shift, a few scattered store receipts, or a bit of commercial surveillance camera footage. But never could the government have successfully assembled a minute-by-minute transcript of a person's long-concluded movements over days, weeks, or months.

Indeed, prior to the digital age, the only way for the government conceivably to have obtained anything close to an "average of 134 data location points per day," *Graham*, 824 F.3d at 447 (Wynn, J., dissenting in part)—or "one location data point every *five and one half minutes*," *Davis*, 785 F.3d at 540 (Martin, J., dissenting)—would have been to ask the

suspect to recall his past movements and divulge them to police. But that exercise would be severely limited by the vagaries of human memory and the Fifth Amendment's privilege against self-incrimination, *see Kastigar v. United States*, 406 U.S. 441, 444-45 (1972).

Accordingly, the power to "reconstruct someone's specific movements down to the minute, not only around town but also within a particular building," *Riley*, 134 S. Ct. at 2490 (citing *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)), gives police access to "a category of information that *never* would be available through the use of traditional law enforcement tools of investigation." *Augustine*, 4 N.E.3d at 865; *see also Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (location information obtained through modern technologies triggers the Fourth Amendment because it offers a never-before-available "precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations").

To be sure, the CSLI at issue here involves historical location data, rather than the real-time tracking that GPS devices provide. But this only strengthens the claim for Fourth Amendment protection. Absent constitutional oversight, the availability of CSLI records would make it "relatively easy and cheap," *Jones*, 565 U.S. at 429 (Alito, J., concurring in the judgment), for the government to pervasively track virtually any American. With uninhibited access to cell phone location data, police would not need to surreptitiously attach a GPS tracker to a target's car, nor return periodically to

covertly change the tracker's batteries. *See, e.g.*, *United States v. Sparks*, 711 F.3d 58, 60 (1st Cir. 2013). The risk of the suspect discovering the surveillance would be zero, and a law enforcement agency would be limited neither by the number of agents in its employ nor the number of tracking devices it could afford. For only a nominal fee to the suspect's service provider—or no fee at all—law enforcement could obtain a detailed journal of a person's locations and movements over a very long period.[7] The available data is limited only by the retention policies of service providers, which are typically long: five years for AT&T, 18 months for Sprint, one year for Verizon.[8]

The ready availability of CSLI makes real the Court's concern in *United States v. Knotts* about "dragnet type law enforcement practices" that make possible "twenty-four hour surveillance of any citizen of this country." 460 U.S. 276, 283-84 (1983) (citation omitted). "When requests for cell phone location

---

[7] Letter from William B. Petersen, Gen. Counsel, Verizon Wireless, to Sen. Edward J. Markey 5 (Oct. 3, 2013), https://www.markey.senate.gov/imo/media/doc/2013-12-09_VZ CarrierResponse.pdf ("In the majority of instances . . . Verizon Wireless does not seek reimbursement for responding to law enforcement requests."); Letter from Charles McKee, Vice President, Sprint Nextel, to Sen. Edward J. Markey 5 (Oct. 3, 2013), http://s3.documentcloud.org/documents/889100/response-sprint.pdf ("Sprint Letter") (charging $30 per hour worked responding to requests for CSLI).

[8] Letter from Timothy P. McKone, Executive Vice President, AT&T, to Sen. Edward J. Markey 3 (Oct. 3, 2013), http://www.markey.senate.gov/imo/media/doc/2013-10-03_ATT_re_Carrier.pdf; Sprint Letter, *supra*, at 2; Silliman, *supra*.

information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that 'such dragnet-type law enforcement practices' are already in use." *United States v. Pineda-Moreno*, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing *en banc*).

c. The reasonableness of the expectation of privacy here is bolstered by protections adopted in federal and state law. In assessing whether an expectation of privacy is objectively reasonable, norms and expectations shaped by federal and state statutes are relevant considerations. *See Florida v. Riley*, 488 U.S. 445, 451 (1989) (plurality opinion) (finding that police surveillance from a helicopter did not invade a reasonable expectation of privacy in part because "the helicopter in this case was *not* violating the law" by flying over private property at an elevation of 400 feet).[9]

Federal law protects the confidentiality of cell phone location data by prohibiting cellular service providers from disclosing sensitive customer records –including "information that relates to the . . . location . . . of use of a telecommunications service"—without "approval of the customer." 47 U.S.C. § 222(c)(1), (h)(1)(A). Congress has recognized

---

[9] Similarly, "[i]n evaluating the reasonableness of police procedures under the Fourth Amendment," this Court has looked to "prevailing rules in individual jurisdictions" and the trend in relevant state laws. *Tennessee v. Garner*, 471 U.S. 1, 15-18 & n.21 (1985) (citing *United States v. Watson*, 423 U.S. 411, 421-22 (1976)).

the particular sensitivity of location information, even beyond the sensitivity of other telecommunications records, by specifying that "a customer shall not be considered to have approved the use or disclosure of or access to . . . call location information" "without [providing] express prior authorization." *Id.* § 222(f). As one of the sponsors of this provision explained, the statute "protects us from Government knowing where you are going and what you are doing in your life." 145 Cong. Rec. H9858–01, at H9860 (daily ed. Oct. 12, 1999) (statement of Rep. Tauzin).[10]

In addition, since 2013 nine states have required law enforcement to obtain a search warrant for historical CSLI by statute or pursuant to judicial interpretation of the state constitution.[11] The high courts of at least seven more states have not yet

---

[10] For assessing reasonable expectations of privacy, the Court looks to the rules governing *public* access to private information or areas, rather than to what law enforcement can do. *See California v. Ciraolo*, 476 U.S. 207, 213-14 (1986); William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv. L. Rev. 1821, 1825-26, 1831 (2016). Thus, the Court in *Ciraolo* looked to whether aerial surveillance by law enforcement took place within legally navigable airspace as determined by federal law, where "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed." 476 U.S. at 213-14 (citing 49 U.S.C. App. § 1304 (current version at 49 U.S.C. § 40103)).

[11] *Commonwealth v. Augustine*, 4 N.E.3d 846 (Mass. 2014); Cal. Penal Code § 1546.1(b); Me. Rev. Stat. tit. 16, § 648; Minn. Stat. §§ 626A.28(3)(d), 626A.42(2); Mont. Code Ann. § 46-5-110(1)(a); N.H. Rev. Stat. Ann. § 644-A:2; 12 R.I. Gen. Laws § 12-32-2; Utah Code Ann. § 77-23c-102(1)(a); Vt. Stat. Ann. tit. 13, § 8102(b); *see also* Kan. Stat. Ann. § 22-2502(a)(1)(G)(i).

addressed CSLI specifically but have recognized a reasonable expectation of privacy in telephone dialing or billing records more generally.[12] Additional states explicitly require a warrant for real-time cell phone location data.[13] In combination, these laws reflect "public attitudes" toward the expectation of privacy in cell phone location records, *see Jones*, 565 U.S. at 429 (Alito, J., concurring in the judgment), and make it reasonable for individuals to expect that their everyday location and movements over an extended period will remain private.

These laws also support a normative judgment that the privacy of this information is integral to living in a free and democratic society. As the Court noted in *Smith v. Maryland*, 442 U.S. at 740 n.5, the reasonable-expectation-of-privacy inquiry includes a normative component, in order to avoid significant erosion of privacy protections central to our constitutional order. Allowing the government to freely obtain the detailed whereabouts of any—or all—of its citizens without a warrant would dramatically "alter the relationship between citizen and government in a way that is inimical to democratic society," *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

---

[12] *See* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373, 396-99 & nn.118-28 (2006) (citing cases from the high courts of, *inter alia*, Colorado, Hawaii, Idaho, Illinois, New Jersey, Pennsylvania, and Washington).

[13] *See Tracey v. State*, 152 So. 3d 504 (Fla. 2014); *State v. Earls*, 70 A.3d 630 (N.J. 2013); 725 Ill. Comp. Stat. 168/10; Ind. Code § 35-33-5-12; Md. Code Ann. Crim. Proc. § 1-203.1(b).

3. Contrary to the Sixth Circuit's reasoning, Pet. App. 14a-15a, acquisition of CSLI intrudes on reasonable expectations of privacy even if CSLI data is sometimes less precise than GPS data. Any attempt to differentiate between CSLI and GPS information is unsupportable in fact, not administrable in practice, and likely to become obsolete as technology advances.

a. While the CSLI in this case, which reflects the state of the technology in 2010 and 2011, did not generally yield GPS-level precision, it was nonetheless highly revealing. Petitioner's cellular service provider recorded and retained information about the location of petitioner's phone at the start and end of both outgoing and incoming calls. Pet. App. 4a. Each location point in the records identified the wedge-shaped cell site sector in which the phone was located at a particular time. The size of those sectors varied widely. In a sparsely populated rural area, a cell site's coverage area might have extended for miles. Pet. App. 5a. In a dense urban or suburban area, cell sites were (and continue to be) located much closer together—down to a few hundred meters apart or, in the case of small cells, significantly less. Hoy, *supra*, at 69-70, 244.

Accordingly, the prosecution used petitioner's CSLI to demonstrate that he was "right where the first robbery was at the exact time of the robbery, the exact sector," J.A. 131, and that he was "right in the right sector before the Radio Shack in Highland Park," J.A. 132. The prosecution also argued that petitioner's phone was in a location on December 13, 2010, "consistent with the geographic area that encompasses the robbery scene," J.A. 58, and that his

location data provided "corroboration" to other evidence in the case, J.A. 131.

b. Even comparatively less precise location information can enable law enforcement to infer the exact location of a phone inside a home or other building. For example, "the Government has asserted in other cases that a jury should rely on the accuracy of the cell tower records to infer that an individual, or at least her cell phone, was at home." *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't* (*Third Circuit CSLI Opinion*), 620 F.3d 304, 311-12 (3d Cir. 2010); *accord Davis*, 785 F.3d at 540-41 (Martin, J., dissenting) (same). The government has used CSLI to place defendants "literally right up against the America Gas Station immediately preceding and after [the] robbery occurred," *Davis*, 785 F.3d at 541 (Martin, J., dissenting) (alteration in original) (quoting trial transcript), "literally . . . right next door to the Walgreen's just before and just after that store was robbed," *id.* (alteration in original), and "right close to the McDonalds" before the robbery of that business, Trial Tr. of Apr. 27, 2012 at 96, *United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012) (No. RDB-11-0094), *aff'd* 824 F.3d 421 (4th Cir. 2016), *petition for cert. filed*, No. 16-6308.

CSLI reveals not just where a person was at discrete moments, but where she was going. In this case, the government presented testimony explaining that cell site data points revealed petitioner's trajectories placing him at certain businesses at the relevant times. *See* J.A. 59, 61-62, 66-67; *see also United States v. Stimler*, __ F.3d __, 2017 WL

3080866, at *16 (3d Cir. July 7, 2017) (Restrepo, J., concurring in part) ("The [government] expert also used CSLI to describe an individual's 'southbound movement on I-278.'"). And CSLI even allows the government to learn with whom a person associated and when, by matching the location information of two or more individuals. *See, e.g.*, Pet. App. 81a-82a (concluding that petitioner and his co-defendant were at the same location based on their CSLI records); J.A. 133 (same).

Finally, cell site location information can "identify various patterns of life"[14] and "identify important places in people's lives" such as their home and work.[15] When paired with other information about phone calls and text messages stored by service providers, it can even facilitate prediction of a cell phone user's personality traits.[16]

c. Regardless of the precise granularity of the technology used in this case, "the rule [the Court]

---

[14] Neal Walfield et al., *A Quantitative Analysis of Cell Tower Trace Data for Understanding Human Mobility and Mobile Networks*, 6th International Workshop on Mobile Entity Localization, Tracking and Analysis 8 (Oct. 10, 2016), https://hal.inria.fr/hal-01378622/document.

[15] Sibren Isaacman et al., *Identifying Important Places in People's Lives from Cellular Network Data*, Proc. of 9th International Conference on Pervasive Computing 2 (June 2011), http://kiskeya.org/ramon/work/pubs/pervasive11.pdf.

[16] Rodrigo de Oliveira et al., *Towards a Psychographic User Model from Mobile Phone Usage*, Proceedings of the ACM CHI 2011 Conference on Human Factors in Computing Systems 2195 (2011), http://www.ic.unicamp.br/~oliveira/doc/CHI2011-WIP_Towards-a-psychographic-user-model-from-mobile-phone-usage.pdf.

adopt[s] must take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U.S. at 36. And today, "the proliferation of . . . cell towers has resulted in smaller coverage areas and CSLI that is far more accurate—in some cases as good as GPS." *Stimler*, 2017 WL 3080866, at *17 (Restrepo, J., concurring in part) (internal quotation marks and citation omitted). As one expert in cellular infrastructure has explained, "the precision of [CSLI] data will vary widely for any given customer over the course of a given day, from the relatively less precise to the relatively very precise . . . . For a typical user, over time, some of that data will inevitably reveal locational precision approaching that of GPS."[17]

Cellular service providers can now calculate the "approximate distance the [cell phone] is from the cell site," instead of just logging which sector it is in. Silliman, *supra*. In addition, providers are increasing their network coverage by deploying low-power "small cells," sometimes called "microcells," "picocells," and "femtocells," which provide service to much smaller areas than traditional cell sites. Hoy, *supra*, at 69-70; *Graham*, 824 F.3d at 448 (Wynn, J., dissenting). The number of small cells in the United States now exceeds the number of traditional cell

---

[17] *The Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism & Homeland Sec. of the H. Comm. on the Judiciary*, 113th Cong. 15 (2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania), https://judiciary.house.gov/wp-content/uploads/2016/02/Blaze-Testimony.pdf.

sites.[18] Callers connecting to a carrier's small cells can be located to a high degree of precision, "such as one floor of a building, the waiting room of an office, or a single home." *Graham*, 824 F.3d at 448 (Wynn, J., dissenting).[19]

CSLI is also becoming more voluminous. Cellular service providers now collect and retain location information not just for the start and end of calls, but for text messages and data connections, "such as checking email, watching a video, or using apps." Silliman, *supra*; *see also* Hoy, *supra*, at 255. During internet-based data connections, service providers "collect[] multiple location points." Silliman, *supra*. Americans "spend two hours and 32 minutes a day[,] on average, using apps or accessing the web on their smartphones—a figure that has doubled in the past year alone." CTIA, *Wireless Snapshot 2017*, at 4 (2017).[20] Even when people are not actively using their phones, many email and social media apps regularly contact the network to

---

[18] *Compare* Michael Carroll, *Small Cells Hit Milestone*, FierceWireless, Nov. 1, 2012, http://www.fiercewireless.com/europe/small-cells-hit-milestone (noting Sprint's deployment of one million femtocells in the United States as of 2012), *with* CTIA, *Annual Wireless Industry Survey* (2017), *supra*, at 5 (301,779 traditional cell sites erected by all U.S. cellular carriers as of 2012).

[19] Wireless providers are able to identify the location of small cells in order to comply with emergency calling location requirements (E-911). *See* Fourth Report & Order 18 & n.94, *In re Wireless E911 Location Accuracy Requirements*, PS Docket No. 07-114 (F.C.C. Jan. 29, 2015), https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-9A1.pdf.

[20] https://www.ctia.org/docs/default-source/default-document-library/ctia-wireless-snapshot.pdf.

check for new messages, thus generating a steady stream of location data that would easily eclipse the 101 location points per day represented in petitioner's records. *See* 6th Cir. Doc. No. 29, at 9. This trend toward greater precision and more comprehensive tracking is sure to continue.

Thus, a rule that protects GPS data but not CSLI is doomed to obsolescence and would render the protection established in *Jones* a dead letter. The GPS data at issue in *Jones* itself lacked pinpoint precision, establishing the vehicle's location within only 50 to 100 feet. *Jones*, 565 U.S. at 403. Some CSLI data points already approach this level of precision, and the precision of CSLI will only increase. Indeed, service providers are already able to precisely locate phones in real time by triangulating their location based on signals received from multiple nearby towers. *See In re Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 532-34 (D. Md. 2011).[21]

4. Because "the duration of the period for which historical CSLI is sought will be a relevant consideration in the reasonable expectation of

---

[21] When the government requests historical CSLI it has no way to know in advance how many data points will be for small cells or geographically small sectors, or will otherwise reveal especially precise location information. Nor will it know how frequently a suspect uses his phone, and thus what volume of location data is available. As this Court observed in *Kyllo*, "[n]o police officer would be able to know in advance whether his through-the-wall surveillance picks up 'intimate' details—and thus would be unable to know in advance whether it is constitutional." 533 U.S. at 39. Only clear guidance from this Court will provide adequate constitutional protection.

privacy calculus," there is "some period of time for which the [government] may obtain a person's historical CSLI [free from Fourth Amendment scrutiny], because the duration is too brief to implicate the person's reasonable privacy interest." *Augustine*, 4 N.E.3d at 865; *see also Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment). As in *Jones*, however, the Court "need not identify with precision the point at which" the duration of CSLI constitutes a search. "[T]he line was surely crossed" in this case well before the 127-day mark. *Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment); *see also United States v. Place*, 462 U.S. 696, 709-10 (1983) (holding that the seizure and detention of a traveler's luggage was too lengthy to qualify as "brief" under *Terry v. Ohio*, 392 U.S. 1 (1968), but declining to set a precise time limit for such detentions).

When the time comes to provide precise guidance to law enforcement agents and lower courts, this Court will have ample authority to do so. Across several realms of constitutional criminal procedure, the Court has not hesitated to set bright-line durational limits in order to "provide some degree of certainty [to law enforcement that its conduct] . . . fall[s] within constitutional bounds." *Cty. of Riverside v. McLaughlin*, 500 U.S. 44, 56 (1991) (requiring a judicial determination of probable cause within 48 hours of arrest); *see also, e.g.*, *Maryland v. Shatzer*, 559 U.S. 98, 110 (2010) (holding that once a suspect has invoked his right to counsel, police may not restart custodial questioning for 14 days); *Baldwin v. New York*, 399 U.S. 66, 69 (1970) (holding that the right to a jury trial is triggered whenever the charged offense is punishable

by more than six months' confinement). In the context of historical CSLI, the durational limit should recognize that police would previously have been able to obtain a small quantity of historical location information by canvassing witnesses and collecting other evidence near the scene of a crime, but never could have compiled a minute-by-minute accounting of a suspect's locations over days, weeks, or longer. Drawing a line that protects against collection of longer-term location records is crucial to preserving the privacy that Americans enjoyed from the Framing to the dawn of the digital age.[22]

---

[22] It is also critical to ensure that the line between short term and long term in the context of CSLI does not provide law enforcement a means of evading the durational protection that *Jones* establishes. *Jones*, 565 U.S. at 429-30 (Alito, J., concurring in the judgment). Lower courts applying *Jones* to real-time cell phone location tracking have concluded that tracking for periods ranging from seven hours to four days does not constitute longer-term surveillance under the Fourth Amendment. *See United States v. Riley*, 858 F.3d 1012, 1018 (6th Cir. 2017) (seven hours); *United States v. Wigginton*, No. 6:15-CR-5-GFVT-HAI-1, 2015 WL 8492457, at *4 (E.D. Ky. Dec. 10, 2015) (24 hours); *United States v. Skinner*, 690 F.3d 772, 780 (6th Cir. 2012) (three days); *Ford v. State*, 477 S.W.3d 321, 334-35 (Tex. Crim. App. 2015) (four days). *But see Tracey v. State*, 152 So. 3d 504, 520 (Fla. 2014) (real-time cell phone location tracking is a search, regardless of duration). Only one court has drawn a line in the context of historical cell site location records, and it has concluded (as a matter of state constitutional law) that anything more than six hours is long term and therefore a search. *Commonwealth v. Estabrook*, 38 N.E.3d 231, 237 (Mass. 2015).

B. Law Enforcement Access To Cell Site Location Information Interferes With The Security Of A Person's Private "Papers."

A property-based analysis under the Fourth Amendment provides an independent ground for holding that the government conducts a search (or seizure) when it obtains a person's CSLI.

As this Court made clear in *Jones*, "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*," property-based conceptions of Fourth Amendment rights. *Jones*, 565 U.S. at 409; *see also Florida v. Jardines*, 133 S. Ct. 1409, 1415-16 (2013). Thus, a search necessarily occurs whenever the government intrudes without consent on a person's "papers" or "effects" through trespass or seizure for purposes of gathering information. *See Jones*, 565 U.S. at 406 (citing U.S. Const. amend. IV).

Determining whether the government has interfered with the security of papers or effects within the meaning of the Fourth Amendment requires reference to some external source of law that defines a person's right to exclude others from those papers or effects—be it common-law trespass and property principles, *id.* at 404-05 & n.2, or positive law, *see* William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv. L. Rev. 1821 (2016); Richard M. Re, *The Positive Law Floor*, 129 Harv. L. Rev. F. 313 (2016). Where a source of law protects against access by the *public* without consent, the Fourth Amendment protects against unreasonable access by the *government* as well. Baude & Stern, 129 Harv. L.

Rev. at 1825-26. That is why this Court concluded in *Jardines* that because members of the public lack an implied license under common-law principles to enter and remain on a home's curtilage with a drug-sniffing dog, police officers implicate the Fourth Amendment when engaging in that same conduct. 133 S. Ct. at 1415-16.

Here, the federal Telecommunications Act designates cell phone location information as "customer proprietary network information" ("CPNI")—a category of records that the service provider cannot disclose absent "approval of the customer." 47 U.S.C. § 222(c)(1)-(2), (h)(1)(A). As the Federal Communications Commission explains, location information "clearly qualifies as CPNI," and therefore subjects service providers to "a duty to protect [its] confidentiality." *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 28 FCC Rcd. 9609, 9616, 9619 ¶¶ 22, 29 (2013).

Originally enacted in 1996, the CPNI provision was amended in 1999 to explicitly protect cell phone location information by prohibiting service providers from using or disclosing it "without the express prior authorization of the customer." 47 U.S.C. § 222(f); *see also* Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, § 5, 113 Stat. 1286, 1288. The statute provides a mechanism for people to enforce their right to protect their location information against dissemination without consent, in the form of a civil remedy against service providers. 47 U.S.C. § 207. Congress erected yet more

protections for cell phone location data in 2007 when it made it a crime for any person to obtain or attempt to obtain that information by fraudulent means. 18 U.S.C. § 1039(a), (h)(1)(A); *see also* Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, § 3(a), 120 Stat. 3568, 3569. Thus, as cell phone technology has become more advanced and more widely adopted, Congress has increasingly legislated safeguards against nonconsensual dissemination of CSLI.

The proprietary interest created by statute makes clear that CSLI is the "paper" or "effect" of the customer. "[T]o the extent CPNI is property, . . . it is better understood as belonging to the customer, not the carrier."[23] By restricting the use and transfer of CSLI without consent of the customer, the Telecommunications Act grants that customer a right to exclude others from it. As required by federal regulations, service providers take concrete steps to guarantee that right: During petitioner's time as a MetroPCS customer, for example, that company would release a subscriber's CPNI only to that subscriber, and only "upon the subscriber's provision of the correct password" over the phone or "presentation of valid identification" during an in-person request. MetroPCS, Annual 47 C.F.R. § 64.2009(e) CPNI Certification, EB Docket 06-036 (Mar. 1, 2011), https://ecfsapi.fcc.gov/file/7021032829.pdf. Accordingly, the government's obtaining of

---

[23] Second Report & Order and Further Notice of Proposed Rulemaking, *In re Implementation of the Telecommunications Act of 1996*, 13 FCC Rcd. 8061, at *14 (1998), *vacated on other grounds by U.S. West, Inc. v. F.C.C.*, 182 F.3d 1224 (10th Cir. 1999).

personal CSLI information invades individuals' "papers" and "effects," and constitutes a search.

C. Pre-Digital Cases Concerning The Third-Party Doctrine Do Not Govern This Case.

1. Cell Site Location Information Is Far More Sensitive Than the Phone and Bank Records Involved in *Smith* and *Miller*, and Unlike Those Records, Is Not Voluntarily Conveyed.

The Sixth Circuit believed that two cases from the pre-digital age—*Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976)—constituted "binding precedent" precluding application of the Fourth Amendment to the records at issue. Pet. App. 12a-14a; *see also* BIO 14. They do not. There is no basis in this Court's jurisprudence for extending *Smith* and *Miller* to CSLI, both because the information is more sensitive, and because it is not voluntarily shared with a third party in any meaningful way.

In *Smith*, this Court ruled that the use of a pen register for several days to capture the telephone numbers a person dials does not implicate a reasonable expectation of privacy. 442 U.S. at 740-42. The Court assessed the degree of invasiveness of the surveillance to determine whether the caller had a reasonable expectation of privacy, noting the "pen register's limited capabilities" and explaining that "a law enforcement official could not even determine from the use of a pen register whether a communication existed." *Id.* at 741-42 (citation

omitted). The Court emphasized that when dialing a phone number, the caller "voluntarily convey[s] numerical information to the telephone company." *Id.* at 744. People must know this, the Court explained, because they have to "convey" phone numbers to the phone company in the process of dialing them, and because "they see a list of their long-distance (toll) calls on their monthly bills." *Id.* at 742.

Similarly, in *Miller* the Court concluded that a bank customer lacked any Fourth Amendment interest in several months' worth of canceled checks, deposit slips, and account statements held by a bank. 425 U.S. at 438, 440. The Court explained that "[w]e must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents." *Id.* at 442. The Court concluded that there was a low privacy interest in the records, because "[t]he checks are not confidential communications but negotiable instruments to be used in commercial transactions." *Id.* As in *Smith*, the Court also noted that the government obtained "only information voluntarily conveyed to the banks." *Id.*

This Court need not disturb the holdings of *Smith* and *Miller* to conclude that they do not apply in this context. The particular records at issue here are far more sensitive and personal than those in *Smith* and *Miller*, and are not conveyed in a meaningfully voluntary way. Indeed, the typical user is not even aware that the cellular service provider has this compendium of sensitive information.

a. The degree of sensitivity in the information here is alone sufficient to distinguish *Smith* and

Miller. That is the teaching of the concurrences in *Jones*. Before that case, this Court had applied *Smith* to hold that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another" because he "voluntarily convey[s] to anyone who want[s] to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination." *Knotts*, 460 U.S. at 281-82. But in *Jones*, five Justices concluded that longer-term surreptitious GPS monitoring of cars traveling on public streets violates reasonable expectations of privacy. Longer-term GPS information is so personally sensitive and so unlikely to have been obtained in the pre-digital era that it triggers a reasonable expectation of privacy, regardless of whether the locational information it contains was theoretically disclosed to the entire public at large.

Indeed, to assess individuals' expectations of privacy in records or information held by a third party, this Court has *never* relied simply on the fact that they were shared, but has also looked to what privacy interest a person has in the information the records reveal. *See, e.g.*, *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (reasonable expectation of privacy in diagnostic test records held by hospital); *Stoner v. California*, 376 U.S. 483, 485, 489-90 (1964) (Fourth Amendment protects privacy in hotel room even though a guest "undoubtedly gives implied or express permission to such persons as maids, janitors or repairmen to enter his room in the performance of their duties" (internal quotation marks and citation omitted)). Far from being a formalistic rule, the "third party" doctrine is really

just a shorthand for one factor in the overall reasonable-expectation-of-privacy analysis—a factor that can be overcome when highly sensitive information is at stake.

That is the case here. Just as in *Jones* and *Riley*, "any extension of [pre-digital] reasoning to digital data has to rest on its own bottom." *Riley*, 134 S. Ct. at 2489. Here, the 186 pages of cell phone location records covering four months are orders of magnitude more granular and revealing than the records in *Smith* and *Miller*. Equating a comprehensive digital repository of cell phone location records with a few days of dialed telephone numbers or even several months' worth of canceled checks "is like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Riley*, 134 S. Ct. at 2488. Both are records in the possession of a third party, "but little else justifies lumping them together." *Id.*

It is no answer to assert, as the Sixth Circuit did, that CSLI cannot be protected under the Fourth Amendment because it does not reveal "the *content* of personal communications." Pet. App. 9a-11a (emphasis added). Though this Court has "occasionally described" its conclusions in terms of contents of communications, it has "never suggested that this concept can serve as a talismanic solution to every Fourth Amendment problem." *Katz*, 389 U.S. at 351 n.9 (citations omitted). *Jones* illustrates as much: GPS information is nothing more than a record of movements; it does not convey any substantive content of personal communications. And yet five Justices have concluded that the Fourth Amendment protects it under the reasonable-

expectation-of-privacy test. *See also Kyllo*, 533 U.S. at 36 (extending Fourth Amendment protection to use of a thermal imaging camera to observe heat emanating from a house, even though an inferential step is required to deduce sensitive information about the interior of the home).

b. *Smith* and *Miller* also do not control because there is no meaningfully voluntary conveyance of CSLI. The act of possessing a cell phone, and even more so the transmission of location information, is not voluntary in any meaningful way.

i. The government asserts that any person who "cho[o]se[s] to carry a cell phone" "takes the risk" that her service provider will reveal days, weeks, or months of her location information to the government. BIO 16. Under this theory, the "choice" that exposes a person's location history to warrantless search is not the knowing placement of a call or sending of a text message, but any possession of a cell phone. Location information is generated not only for outgoing communications initiated by the phone user, but also for *incoming* calls (whether answered or not) and text messages, and for countless data connections made without any active participation of the user, such as when a phone sitting in a person's pocket or purse checks every few seconds or minutes for new emails or social media updates.

The mere act of possessing a cell phone does not voluntarily disclose a comprehensive record of one's movements in any meaningful sense. Modern cell phones are "a pervasive and insistent part of daily life." *Riley*, 134 S. Ct. at 2484. Virtually every American adult has a cell phone, and people feel

compelled to carry their cell phones with them nearly everywhere they go, serving as "necessary instruments for self-expression, even self-identification." *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010). Many employers also demand that people remain digitally "in touch" at all times—or at least when away from the office during normal business hours.

Alternative means of enabling this type of communication are fast disappearing—or never existed in the first place. A majority of American homes now do not have a landline telephone, as residents rely exclusively on cell phones.[24] The number of pay phones in the United States has plummeted from more than two million in 1997, to less than 100,000 today.[25] And no other device—past or present—allows people to text, email, check social media, and follow daily political announcements while away from home or the office. In short, smartphones are "not just another technological convenience"; they have become indispensable for full participation in family, social, professional, civic, and political life. *Riley*, 134 S. Ct. at 2494.

Furthermore, cell phones are now vital instruments of personal safety. For many, they are

---

[24] Stephen J. Blumberg & Julian V. Luke, Ctrs. for Disease Control & Prevention, Nat'l Ctr. for Health Statistics, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July–December 2016* 1 (2017), https://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201705.pdf.

[25] F.C.C., Indus. Analysis & Tech. Div., *Payphone Data from 1997 Through 2016* tbl.1 (2017), https://www.fcc.gov/file/12198/download.

the exclusive means to call first responders, physicians, or family members in a medical emergency or to report a crime; to seek roadside assistance or summon police after a car accident, flat tire, or vehicle breakdown; to get directions when lost; and to check on the whereabouts of a child. "[A]bout 70 percent of 911 calls are placed from wireless phones, and that percentage is growing. For many Americans, the ability to call 911 for help in an emergency is one of the main reasons they own a wireless phone." F.C.C., *911 Wireless Services*.[26] Ready access to a functioning cell phone provides a level of security that most Americans cannot realistically give up.

Finally, smartphones are fast gaining capacity to be used as critical medical instruments. New software allows them to monitor bodily functions and transmit data to doctors in real time. Eric J. Topol, *The Future of Medicine Is in Your Smartphone*, Wall St. J., Jan. 9, 2015.[27] If a person's doctor instructs her to carry a smartphone to monitor her heart rate or the amount of a certain chemical in her bloodstream, following that instruction can hardly be considered a "voluntary" act that assumes the risk that the government might track the person's every movement. The same is true of an equivalent request

---

[26] https://www.fcc.gov/consumers/guides/911-wireless-services. *See also* Pew Research Ctr., *U.S. Smartphone Use in 2015* 25 (2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015 ("Fully 53% of smartphone owners indicate that they have been in an emergency situation where having their phone available helped resolve the situation.").

[27] https://www.wsj.com/articles/the-future-of-medicine-is-in-your-smartphone-1420828632.

from one's employer that one remain in touch and available while away from the office. People should not be forced to choose between their privacy and their safety, health, or livelihood.

This is especially so because each of a smartphone's essential functions—calling, texting, emailing, data access, navigation, medical monitoring, and so on—is impossible to use without leaving a trail of location records held by the service provider. There is no way to avoid the aggregation and retention of this location information short of turning off or disabling the phone.

Most smartphones have a location privacy setting that, when enabled, prevents applications ("apps")—such as a GPS navigation app—from accessing the phone's location. *See, e.g.*, Apple, *iPhone User Guide: Location Services*.[28] Users might well believe that enabling this function protects their locational privacy. But this setting has no impact at all upon cellular service providers' ability to log and retain the phone's location. Maxwell Payne, *How to Turn Off GPS on a Cell Phone*, USA Today.[29] Virtually any use of the phone generates a location record. There is no option to close the proverbial phone booth door. *See Katz*, 389 U.S. at 352.

ii. Even if the *possession* of cell phones could be said to be voluntary, the *conveyance of location information* of the type obtained by the government here surely cannot. Though some people may have a

---

[28] https://help.apple.com/iphone/10/#/iph3dd5f9bc.

[29] http://traveltips.usatoday.com/turn-off-gps-cell-phone-21147.html.

general sense that their cell phones must communicate with the service provider's cell towers in order to place and receive calls, they cannot know whether the service provider is logging and retaining that data and in what form or detail: single-tower data or triangulated position; sector information or estimated distance from the nearest cell site. People do not know which cell tower and sector their phone is connected to at any time, how large the coverage area of that tower is, or how long the carrier retains location records. Nor will they know whether their phone was roaming on another carrier's network, as was petitioner's here, Pet. App. 72a, and thus whether a company with which they have no contractual relationship whatsoever is logging and retaining their location. *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011, 1028-29 (N.D. Cal. 2015).

It is also telling that, unlike in *Smith* and *Miller*, individuals do not receive their CSLI in their monthly bill. *Compare Smith*, 442 U.S. at 742, *with Graham*, 824 F.3d at 445 (Wynn, J., dissenting in part). Even a customer who *wanted* to learn this information could not do so: service providers refuse to disclose location records to customers who request them. Megha Rajagopalan, *Cellphone Companies Will Share Your Location Data – Just Not With You*, ProPublica, June 26, 2012.[30]

Put another way, people do not knowingly or intentionally convey to their service provider a "virtual current biography," *People v. Blair*, 602 P.2d

---

[30] https://www.propublica.org/article/cellphone-companies-will-share-your-location-data-just-not-with-you.

738, 745 (Cal. 1979), charting their locations and movements over weeks and months. While people may know in some general sense that they have to be near a cell tower in order to make or receive a call, it would be outlandish to extrapolate from that minimum knowledge the conclusion that people knowingly and voluntarily disclose their every movement to the government. There is a huge difference between the knowing act of using a cell phone to make a discrete communication, and the involuntary and generally unknown process by which thousands of individual location points are aggregated into a digital almanac of a cell phone user's life.

2. Extending *Smith* and *Miller* to CSLI Records Would Remove a Great Volume of Other Similarly Sensitive Digital Records from the Protection of the Fourth Amendment.

Although it may someday be necessary to "reconsider the premise" of the third-party doctrine, *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring), it is not necessary in this case to reassess its continued validity in every possible context. Properly understood, the disclosure of information to a third party is but one factor in determining whether a reasonable expectation of privacy exists. *See supra* Part I.C; *see also State v. Walton*, 324 P.3d 876, 901 (Haw. 2014). And this Court has explained that "[i]t would be foolish" to suggest that such Fourth Amendment analyses should not account for "the advance of technology." *Kyllo*, 533 U.S. at 33-34. These principles are sufficient to resolve this case.

At the same time, were the Court to hold that the mere act of disclosing information to a third-party business is enough to defeat any Fourth Amendment protection, it would not only effect "a significant diminution of privacy," *Riley*, 134 S. Ct. at 2493, but would also throw into question whether a vast array of Americans' most highly sensitive records can be be protected in the 21st century against dragnet access at law enforcement's whim. Indeed, under the government's theory, people would have no reasonable expectation of privacy even in their emails, because the contents of those communications are shared with a third party.

"In our time, unless a person is willing to live 'off the grid,' it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life." *Davis*, 785 F.3d at 525 (Rosenbaum, J., concurring). People cannot avoid disclosing "the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers[,]the books, groceries, and medications they purchase to online retailers," *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring), the contents of their emails, text messages, and private social media communications to their electronic communication service providers, their search queries to Google, their GPS coordinates and location history to Apple, Google, and Waze, their intimate photos to Apple or Flickr, and their medical queries to WebMD. *See Davis*, 785 F.3d at 536 (Martin, J., dissenting).

Moreover, with the rapid proliferation of the so-called "internet of things," virtually any appliance

or effect can now be connected to the internet and programmed to transmit information about a person's home, body, or movements to a third-party company's cloud-based server. Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 Cal. L. Rev. 805 (2016). Even detailed information about "exercise, moods, sleep patterns, and food intake," *id.* at 818, reproductive health,[31] and sexual activity[32] is now recorded and retained on servers controlled by a third party. Not even utterances within the walls of a home are exempt.[33]

Under the government's theory, this vast array of information would automatically lose Fourth Amendment protection. The Sixth Circuit tried to erect a barricade against such slippage, holding that persons have a reasonable expectation of privacy in the "contents" of communications, such as emails. *United States v. Warshak*, 631 F.3d 266, 285-88 (6th Cir. 2010). But if the Sixth Circuit and the government are correct that *Smith* and *Miller* "resolve this case" because "'a person has no

---

[31] *See* Moira Weigel, *'Fitbit for Your Period': The Rise of Fertility Tracking*, Guardian, Mar. 23, 2016, https://www.theguardian.com/technology/2016/mar/23/fitbit-for-your-period-the-rise-of-fertility-tracking.

[32] *See* Kashmir Hill, *This Sex Toy Tells the Manufacturer Every Time You Use It*, Fusion, Aug. 9, 2016, *available at* https://web.archive.org/web/20170507193448/https://fusion.kinja.com/this-sex-toy-tells-the-manufacturer-every-time-you-use-1793861000.

[33] *See* Tim Moynihan, *Alexa and Google Home Record What You Say. But What Happens to that Data?*, Wired, Dec. 5, 2016, https://www.wired.com/2016/12/alexa-and-google-record-your-voice.

legitimate expectation of privacy in information he voluntarily turns over to third parties,'" BIO 14-15 (quoting *Smith*, 442 U.S. at 743-44), there is no way to distinguish emails—or any other of the data just described—from CSLI.[34] Surely a world in which people could not treat their email communications as private would be a radical departure from the privacy people have long expected with respect to their letters, phone calls, and now electronic communications.

II. SEARCHING CELL SITE LOCATION INFORMATION IS UNREASONABLE WITHOUT A WARRANT.

Though issued by neutral magistrates, the orders that enabled the government to procure petitioner's CSLI were made upon an assertion of "specific and articulable facts showing that there are reasonable grounds to believe that" the records were "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d); Pet. App. 53a. That showing is well short of the probable cause required for a warrant. As the government explained below, "reasonable grounds is less than probable

---

[34] The government has also analogized CSLI to the records in *Smith* and *Miller* on the ground that CSLI data are "business records" that service providers "create for their own purposes." BIO 14. But as explained *infra* at Part II.B, CSLI does not constitute a "business record" in any traditional sense. In any event, this Court should eschew any rule that would hinge Fourth Amendment protection on whether information constitutes a "business record." That term has no established meaning, and is untethered from the relevant Fourth Amendment inquiry: whether there is a reasonable expectation of privacy or a property interest in the records at issue.

cause. . . . [and] reasonable grounds to believe that something is relevant . . . is . . . another gigantic qualification, [because] what might be relevant to something can be really far afield." J.A. 34. In the government's view, government agents do not even "have to show a crime. We merely have to show there's a criminal investigation of a crime." *Id.* And unlike a warrant, an application under section 2703(d) does not require a sworn affidavit from the investigating officer, but is issued upon the assertions of a prosecutor in an unsworn application.

The government nevertheless advances three reasons why the Court should find its warrantless search reasonable: that Congress's 30-year-old mechanism for obtaining a court order without probable cause deserves deference; that this Court's cases involving subpoenas automatically render warrantless searches of records held by businesses reasonable; and that a balancing of law enforcement interests against the privacy invasion at issue renders the warrant requirement unnecessary. *See* BIO 22-26.

Because the Sixth Circuit concluded that the government's acquisition of petitioner's CSLI was not a Fourth Amendment search, it did not address whether the warrantless search of that information was unreasonable. The Court may therefore wish to resolve only the threshold question of whether there was a search, and allow the court of appeals on remand to address in the first instance whether the search conducted by the government was reasonable. *See Cutter v. Wilkinson*, 544 U.S. 709, 718 n.7 (2005) ("[W]e are a court of review, not of first view."); *cf. Jones*, 565 U.S. at 413.

Should the Court wish, however, to reach the question whether the search was reasonable, it should hold that a warrant is required for law enforcement requests for longer-term CSLI. Where an individual has a reasonable expectation of privacy in an item or location to be searched, the search is "*per se* unreasonable under the Fourth Amendment" unless conducted pursuant to a judicial warrant supported by probable cause. *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz*, 389 U.S. at 357); *accord Quon*, 560 U.S. at 760; *City of L.A. v. Patel*, 135 S. Ct. 2443, 2452 (2015). Only if one of the "few specifically established and well-delineated exceptions" to the warrant requirement applies may government officials conduct a warrantless search. *Gant*, 556 U.S. at 338 (internal quotation marks omitted). Because no exception applies here, search of longer-term historical CSLI pursuant to an order issued on a showing well short of probable cause and lacking in particularity is unreasonable.

A. Congress Has Not Had An Opportunity To Consider This Problem.

The government suggests, and the Sixth Circuit asserted, that "Congress has specifically legislated" on the question of what type of process should govern law enforcement access to CSLI. Pet. App. 15a; *see also* BIO 24. This assertion is mistaken. When Congress enacted the Stored Communications Act in 1986, it neither intended to address nor even considered CSLI, much less whether obtaining longer-term CSLI should require a warrant. Consequently, no deference to this outdated legislative scheme is warranted with respect to CSLI.

In 1986, less than one half of one percent of Americans had a cell phone.[35] There were a mere 1,531 cell sites in the United States (compared to more than 300,000 today).[36] Congress gave no indication that it was aware of the existence of historical CSLI, not to mention that the data would eventually exist as to nearly every American. *See* S. Rep. No. 99-541 (1986); H.R. Rep. No. 99-647 (1986).

When Congress amended the SCA in 1994 to clarify the standard for issuance of an order under section 2703(d),[37] only nine percent of Americans had cell phones, and cellular networks were still fragmented and rudimentary, with less than 18,000 cell sites across the country.[38] Again, there is no indication that Congress even considered historical CSLI. *See* H.R. Rep. No. 103-827 (1994). Congress simply did not anticipate the contemporary ubiquity of cell phones and the volume and precision of CSLI that would be retained by service providers. The SCA accordingly provides no guidance on the question whether warrantless search of CSLI is reasonable.[39]

---

[35] *See* CTIA, *Background on CTIA's Wireless Industry Survey* 2 (2014), https://www.ctia.org/docs/default-source/default-document-library/ctia_survey_ye_2014_graphics.pdf.

[36] *Id.*; CTIA, *Annual Wireless Industry Survey* (2017), *supra*, at 4.

[37] Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 207, 108 Stat. 4279 (1994).

[38] *See* CTIA, *Background on CTIA's Wireless Industry Survey* (2014), *supra*, at 2.

[39] Because the Stored Communications Act in the meantime provides a mechanism for obtaining a warrant for records held by service providers, *see* 18 U.S.C. § 2703(c)(1)(A), in holding that a warrant is required, the Court need not find the SCA

B. Analogy To This Court's Subpoena Cases Does Not Render The Search Reasonable.

The government asserts that the court orders used to obtain petitioner's CSLI are "constitutionally reasonable, because the SCA provides more substantial privacy protections than an ordinary judicial subpoena" by requiring "specific and articulable facts" showing "relevan[ce] and material[ity] to an ongoing criminal investigation," not just a mere assertion of relevance. BIO 24 (quoting 18 U.S.C. § 2703(d)). However, because petitioner has a reasonable expectation of privacy in the records at issue, the government's reliance on the Court's subpoena cases is misplaced.

This Court has held that the government may use administrative subpoenas to procure certain business records and personal records held by third parties. *See Okla. Press Publ'g Co. v. Walling*, 327 U.S. 186, 209 (1946); *Miller*, 425 U.S. at 442-44; *Couch v. United States*, 409 U.S. 322, 336 (1973); *United States v. Powell*, 379 U.S. 48, 57 (1964); *see generally* Christopher Slobogin, *Subpoenas and Privacy*, 54 DePaul L. Rev. 805, 815-24 (2005). Because they are heavily regulated, businesses have, if anything, a diminished Fourth Amendment privacy interest in their own business records. *See United States v. Morton Salt Co.*, 338 U.S. 632, 651-52 (1950). And the Court has upheld the use of

---

unconstitutional. *See In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 617 (5th Cir. 2013) (Dennis, J., dissenting).

administrative subpoenas to obtain personal records held by third parties where "there exists no legitimate expectation of privacy." *Couch*, 409 U.S. at 336 & n.19; *accord Miller*, 425 U.S. at 442-43.

This Court, however, has never held that an administrative subpoena directed to a third party is sufficient to procure records in which the individual whom the government is investigating has a reasonable expectation of privacy. Such a holding would radically expand the subpoena power. It would also subvert the core functions of the Fourth Amendment's warrant requirement: to govern criminal investigative searches and seizures and check government overzealousness. *Johnson v. United States*, 333 U.S. 10, 14-15 (1948); *Katz*, 389 U.S. at 356.

In the context of highly sensitive records held by third parties, the requirements of probable cause, particularity, and judicial review that accompany a warrant are crucial mechanisms for preventing violations of individuals' Fourth Amendment rights. Warrants guarantee notice and, in lieu of the target's opportunity to seek to quash the government's request, warrants issue only after a neutral magistrate's independent determination of probable cause and particularity. By contrast, the Stored Communications Act allows requests for CSLI without probable cause, and expressly provides that the government "is not required to provide notice to a subscriber or customer" whose records are requested by subpoena or order. 18 U.S.C. § 2703(c)(3). Indeed, in the context of administrative subpoenas for records lacking a reasonable expectation of privacy, this Court has held that the government need not

notify the investigative target. *S.E.C. v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984).[40]

In cases where the investigative target herself holds the records the government seeks, she can protect her rights by asserting privilege under the Fifth Amendment, *United States v. Hubbell*, 530 U.S. 27 (2000), or by obtaining pre-enforcement judicial review to argue that the subpoena seeks information beyond what is truly relevant to the investigation, *see Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984). But in the context of subpoenas to third parties, there is no Fifth Amendment privilege against production of incriminating information, *Couch*, 409 U.S. at 336, and the third party will often lack the knowledge and incentive to challenge the relevance of a subpoena or its scope. The protections of a warrant, including particularity and probable cause, provide crucial protection against abuse.

C. A Balancing Of Interests Under The Fourth Amendment Commands That A Warrant Is Required.

The government finally argues that the Court should conduct its own general reasonableness inquiry that balances the degree of intrusion on privacy against the strength of the government's interest. BIO 24-26. But as is usually the case, the warrant requirement itself strikes the appropriate

---

[40] Because this case does not involve use of a grand jury subpoena, the Court need not address whether different rules are appropriate for subpoenas issued by a grand jury. *See United States v. R. Enterprises, Inc.*, 498 U.S. 292, 297, 300 (1991) (explaining that "[t]he grand jury occupies a unique role in our criminal justice system," and must be afforded "wide latitude" in its issuance of subpoenas).

Fourth Amendment balance here. *See Camara v. Municipal Ct.*, 387 U.S. 523, 528-29 (1967).

In any event, even if a more general reasonableness analysis were conducted, the government's need for evidence is no greater than in the broad sweep of other searches for which warrants are required, and the privacy interest is high.

1. The government's interest in obtaining historical CSLI in criminal investigations is indistinguishable from its general interest in gathering evidence to investigate crimes. There is, for example, no interest in officer safety, *United States v. Robinson*, 414 U.S. 218, 234 (1973), or accurate identification of arrestees, *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013), that requires jettisoning the warrant requirement. Rather, in this case the government was seeking evidence to inculpate petitioner and eventually convict him at trial. In such cases, this Court has explained that "the warrant requirement is 'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.'" *Riley*, 134 S. Ct. at 2493 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971)).

Indeed, many law enforcement agencies *already* obtain warrants for CSLI as a matter of state law or local policy. In California, Maine, Massachusetts, Minnesota, Montana, New Hampshire, Rhode Island, Utah, and Vermont, state law mandates use of a warrant for historical CSLI. *See supra* note 11. Elsewhere, a number of police departments—including in the County of Hawai'i and City of Honolulu, Hawai'i; Wichita, Kansas;

Lexington, Kentucky; Lincoln, Nebraska; and North Las Vegas, Nevada--have long required a warrant for historical CSLI as a matter of policy. Am. Civil Liberties Union, *ACLU Affiliate Nationwide Cell Phone Tracking Public Records Requests: Findings and Analysis* 3 (2013).[41] Law enforcement agencies in other states are required to get a warrant for real-time cell-phone location data, *see supra* note 13, as are federal authorities in most of the country, *see United States v. Espudo*, 954 F. Supp. 2d 1029, 1035 (S.D. Cal. 2013).

As the practice in these jurisdictions suggests, the warrant requirement is not unduly burdensome in this context. In the words of the California State Sheriffs' Association when explaining its non-opposition to a bill that codified a warrant requirement for historical CSLI in California, a warrant requirement "ensure[s] that the correct balance is struck between the need for law enforcement to obtain information regarding criminal activities from electronic communications and the privacy interests of those who use email and other forms of electronic communication."[42] Since

---

[41] https://www.aclu.org/sites/default/files/field_document/cell_phone_tracking_documents_-_final.pdf.

[42] Letter from Aaron Maguire, Legislative Counsel, Cal. State Sheriff's Ass'n, to Hon. Mark Leno, Cal. State Senate (Aug. 26, 2015), https://www.eff.org/document/california-state-sheriffs-association-remove-opposition-sb-178-calecpa; *see also* Letter from David Bejarano, President, Cal. Police Chiefs Ass'n, Inc., to Hon. Mark Leno, Cal. State Senate (Aug. 24, 2015), https://www.eff.org/files/2015/09/01/califoria_police_chiefs_association_-_sb_178_leno_-_remove_opposition.pdf (bill does not "imped[e] on law enforcement's ability to serve the needs of their communities").

passage of California's law, law enforcement agencies throughout the state have continued to obtain CSLI pursuant to the newly codified warrant standard. *See* Cal. Dep't of Justice, Office of the Attorney Gen., *Electronic Search Warrant Notifications*, *available at* https://openjustice.doj.ca.gov/data (providing data about subset of warrants issued in first quarter of 2017 for cell phone location information).

2. On the other side of the ledger, the privacy interests are high. As detailed above, longer-term CSLI can reveal a great deal of detailed private information. The orders here, for example, are entirely lacking in particularity and sweep in large quantities of sensitive information without adequate cause. In an attempt to place petitioner at the scenes of eight discrete robberies at known times on eight individual days, the government requested five months and obtained four months (127 days) of petitioner's location data comprising thousands of location data points. Pet. App. 7a, 52a. For the vast majority of those days, the government patently lacked probable cause to believe that a crime had even been committed, much less that petitioner was involved in its commission.

A request for months of data is no aberration: according to T-Mobile, which now owns petitioner's service provider, MetroPCS, the average law enforcement request "asks for approximately fifty-five days of records."[43] Other recent cases involve comparable or even greater quantities of data. In one

---

[43] T-Mobile, *Transparency Report for 2013 & 2014*, at 5 (2015), http://newsroom.t-mobile.com/content/1020/files/NewTransparencyReport.pdf.

case, in the course of investigating robberies on six days, the government obtained 221 days (more than seven months) of cell site location information, revealing 29,659 location points for one defendant. *Graham*, 824 F.3d at 446-47 (Wynn, J., dissenting in part). Other cases in the courts of appeals have involved government searches of CSLI covering 67 days, *Davis*, 785 F.3d at 501, 57 days, *Stimler*, 2017 WL 3080866, at *2, and 37 days, *United States v. Williams*, 161 F. Supp. 3d. 846, 849 (N.D. Cal. 2016), *appeal pending sub nom. United States v. Gilton*, No. 16-10109 (9th Cir.).

Acquisition of these durations and volumes of CSLI seriously infringes on personal privacy. "[T]he Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley*, 134 S. Ct. at 2494. "The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Stanford v. Texas*, 379 U.S. 476, 485 (1965) (citation omitted).

In sum, clarifying that a warrant is required will ensure that law enforcement officers can acquire particular spans of location records where there is probable cause that they will provide evidence of criminal conduct. And it will protect records that are not pertinent to the investigation but that can reveal much private information about a person's life. This

Court should provide a "simple" answer to the question presented: "get a warrant." *Riley*, 134 S. Ct. at 2495.

CONCLUSION

For the foregoing reasons, the judgment of the Sixth Circuit should be reversed.

Respectfully submitted,

Nathan Freed Wessler
Ben Wizner
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004

David D. Cole
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
915 15th Street, NW
Washington, D.C. 20005

Cecillia D. Wang
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111

Harold Gurewitz
Counsel of Record
GUREWITZ & RABEN, PLC
333 W. Fort Street, Suite 1400
Detroit, MI 48226
(313) 628-4733
hgurewitz@grplc.com

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
AMERICAN CIVIL LIBERTIES UNION FUND OF MICHIGAN
2966 Woodward Ave.
Detroit, MI 48201

Jeffrey L. Fisher
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305

Dated: August 7, 2017

RECORD AND BRIEFS

FILED
SEP 25 2017

No. 16-402

In the Supreme Court of the United States

TIMOTHY IVORY CARPENTER, PETITIONER

v.

UNITED STATES OF AMERICA

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

BRIEF FOR THE UNITED STATES

NOEL J. FRANCISCO
Solicitor General
Counsel of Record
KENNETH A. BLANCO
Acting Assistant Attorney General
MICHAEL R. DREEBEN
Deputy Solicitor General
ELIZABETH B. PRELOGAR
Assistant to the Solicitor General
JENNY C. ELLICKSON
Attorney
Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

QUESTION PRESENTED

Whether the government's acquisition, pursuant to a court order issued under 18 U.S.C. 2703(d), of historical cell-site records created and maintained by a cell-service provider violates the Fourth Amendment rights of the individual customer to whom the records pertain.

TABLE OF CONTENTS

Page

Opinions below 1
Jurisdiction 1
Constitutional and statutory provisions involved 1
Statement 2
A. Cell-site records and the Stored Communications Act 2
B. The present controversy 5
Summary of argument 11
Argument:
I. The government's acquisition of providers' business records of the towers used to connect petitioner's calls did not constitute a Fourth Amendment search of petitioner 14
A. A cell-phone user has no reasonable expectation of privacy in business records created by his provider documenting the cell sites used to connect his calls 15
1. Petitioner cannot claim a legitimate privacy interest in information about his proximity to cell towers that he disclosed to his cell-service providers 15
2. Petitioner cannot distinguish this Court's cases finding no reasonable expectation of privacy in information conveyed to a third party 23
3. Cell-service providers' use of technology supplies no basis to depart from well-established Fourth Amendment principles 32
B. The government did not obtain the cell-site records by trespassing on a constitutionally protected area 41

Table of Contents—Continued: Page

II. If the government's acquisition of cell-site records was a search of petitioner, it was reasonable under the Fourth Amendment 43
A. Law enforcement agents need not obtain a warrant to conduct searches using compulsory process 44
B. A traditional balancing of interests further supports the constitutionality of a Section 2703(d) order 50
III. Petitioner correctly concedes that the government does not violate the Fourth Amendment by acquiring shorter-term cell-site records 55
Conclusion 58
Appendix A — Constitutional and statutory provisions 1a
Appendix B — Methodology for creating Figure 2 ..... 13a

TABLE OF FIGURES

Figures:
Figure 1: Excerpt from Gov't Ex. 57 (Pet. App. 86a) 25
Figure 2: Illustrative map of buildings in the area 26

TABLE OF AUTHORITIES

Cases:

Application of the U.S. for Historical Cell Site Data, In re, 724 F.3d 600 (5th Cir. 2013) 19, 38, 41
Atwater v. *City of Lago Vista*, 532 U.S. 318 (2001) 30
Blair v. *United States*, 250 U.S. 273 (1919) 17, 34
Branzburg v. *Hayes*, 408 U.S. 665 (1972) 18
California v. *Greenwood*, 486 U.S. 35 (1988) 23

Cases—Continued: Page

Christian Legal Soc'y v. *Martinez*, 561 U.S. 661 (2010) 42
City of Los Angeles v. *Patel*, 135 S. Ct. 2443 (2015) 45
City of Ontario v. *Quon*, 560 U.S. 746 (2010) 28
Countess of Shrewsbury Case, 2 How. St. Tr. 769 (1612) 17
Dalia v. *United States*, 441 U.S. 238 (1979) 49
Donovan v. *Lone Steer, Inc.*, 464 U.S. 408 (1984) 4, 45
Ferguson v. *City of Charleston*, 532 U.S. 67 (2001) 28
Fisher v. *United States*, 425 U.S. 391 (1976) 48
Granfinanciera, S. A. v. *Nordberg*, 492 U.S. 33 (1989) 43
Hodge v. *Talkin*, 799 F.3d 1145 (D.C. Cir. 2015), cert. denied, 136 S. Ct. 2009 (2016) 24
Hoffa v. *United States*, 385 U.S. 293 (1966) 18
Jackson, Ex parte, 96 U.S. 727 (1877) 37
Kastigar v. *United States*, 406 U.S. 441 (1972) 34
Katz v. *United States*, 389 U.S. 347 (1967) 14, 49
Kyllo v. *United States*, 533 U.S. 27 (2001) 14, 33, 34
Maryland v. *King*, 133 S. Ct. 1958 (2013) 43, 44, 50, 51
McPhaul v. *United States*, 364 U.S. 372 (1960) 44
Oklahoma Press Publ'g Co. v. *Walling*, 327 U.S. 186 (1946) 44, 45, 46, 48
Riley v. *California*, 134 S. Ct. 2473 (2014) 32, 33, 34, 43
SEC v. *Jerry T. O'Brien, Inc.*, 467 U.S. 735 (1984) 18, 49
Shades Ridge Holding Co. v. *Commissioner of Internal Revenue*, 23 T.C.M. (CCH) 1665 (1964) 57
Smith v. *Maryland*, 442 U.S. 735 (1979) ..... *passim*
Stoner v. *California*, 376 U.S. 483 (1964) 28
Subpoena Duces Tecum, In re, 228 F.3d 341 (4th Cir. 2000) 48

Cases—Continued: Page

United States v. *Bennett*, 409 F.2d 888 (2d Cir. 1969) 48
United States v. *Caraballo*, 384 Fed. Appx. 285 (4th Cir. 2010) 56, 57
United States v. *Davis*, 785 F.3d 498 (11th Cir.), cert. denied, 136 S. Ct. 479 (2015) 19, 21, 43, 46, 47, 51
United States v. *Di Re*, 332 U.S. 581 (1948) 53
United States v. *Dionisio*, 410 U.S. 1 (1973) 44, 45, 50, 51
United States v. *Gaskins*, 690 F.3d 569 (D.C. Cir. 2012) 56
United States v. *Graham*:
796 F.3d 332 (4th Cir. 2015), rev'd en banc, 824 F.3d 421 (4th Cir. 2016) 29
824 F.3d 421 (4th Cir. 2016), petitions for cert. pending, Nos. 16-6308 & 16-6694 (filed Sept. 26 & Oct. 27, 2016) 19
United States v. *Gramlich*, 551 F.2d 1359 (5th Cir.), cert. denied, 434 U.S. 866 (1977) 56
United States v. *Grubbs*, 547 U.S. 90 (2006) 49
United States v. *Jacobsen*, 466 U.S. 109 (1984) 35
United States v. *Johnson*, 480 Fed. Appx. 835 (6th Cir. 2012) 56
United States v. *Jones*, 565 U.S. 400 (2012) ..... *passim*
United States v. *Knights*, 534 U.S. 112 (2001) 53
United States v. *Knotts*, 460 U.S. 276 (1983) 39
United States v. *Miller*, 425 U.S. 435 (1976) ..... *passim*
United States v. *Morton Salt Co.*, 338 U.S. 632 (1950) 44, 50, 51
United States v. *Nixon*, 418 U.S. 683 (1974) 17, 18
United States v. *R. Enterprises, Inc.*, 498 U.S. 292 (1991) 46

Cases—Continued: Page

United States v. *Reynolds*, 626 Fed. Appx. 610 (6th Cir. 2015), petition for cert. pending, No. 16-8574 (filed Dec. 10, 2015) 52
United States v. *Salerno*, 481 U.S. 739 (1987) 53
United States v. *Warshak*, 631 F.3d 266 (6th Cir. 2010) 38
United States v. *Watson*, 423 U.S. 411 (1976) 54
United States v. *Zadeh*, 820 F.3d 746 (5th Cir. 2016) 48
Virginia v. *Moore*, 553 U.S. 164 (2008) 22, 23
Whren v. *United States*, 517 U.S. 806 (1996) 39
Young v. *Owens*, 577 Fed. Appx. 410 (6th Cir. 2014) 56

Constitution and statutes:

U.S. Const.:
Amend. I 13, 39
Amend. IV ..... *passim*, 1a
Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, Tit. II, § 207(a), 108 Stat. 4292 54
Hobbs Act, 18 U.S.C. 1951(a) 2
Stored Communications Act, 18 U.S.C. 2701 *et seq.* 4
18 U.S.C. 2703 ..... 4, 54
18 U.S.C. 2703(c)(1)(B) 4
18 U.S.C. 2703(d) ..... *passim*, 4a
18 U.S.C. 2707(g) 51
15 U.S.C. 6802 22
18 U.S.C. 924(c) 2
26 U.S.C. 7216 22
47 U.S.C. 222 ..... 21, 22, 42, 7a
47 U.S.C. 222(c)(1) 21, 22, 42
47 U.S.C. 222(d) 21

Statutes—Continued: Page

47 U.S.C. 222(d)(1)-(4) 42
47 U.S.C. 222(f) 22
47 U.S.C. 222(h)(1) 22

Miscellaneous:

AT&T, *AT&T Privacy Policy* (May 2, 2017), http://about.att.com/sites/privacy_policy/full_privacy_policy 3
Digital Privacy Act of 2000, H.R. 4987, 106th Cong., 2d Sess. (2000) 55
Geolocation Privacy and Surveillance Act:
H.R. 1312, 113th Cong., 1st Sess. (2013) 55
H.R. 1062, 115th Cong., 1st Sess. (2017) 55
S. 237, 114th Cong., 1st Sess. (2015) 55
Geolocation Technology and Privacy: Hearing Before the H. Comm. on Oversight and Government Reform, 114th Cong., 2d Sess. (2016) 52
H.R. Rep. No. 647, 99th Cong., 2d Sess. (1986) 53, 54
H.R. Rep. No. 827, 103d Cong., 2d Sess. Pt. 1 (1994) 53
Lennart Norell et al., *Wi-Fi calling—extending the reach of VoLTE to Wi-Fi*, Ericsson Review 1 (Jan. 30, 2015), https://www.ericsson.com/res/thecompany/docs/publications/ericsson_review/2015/er-wifi-calling.pdf 27
Pew Research Ctr., *Public Perceptions of Privacy and Security in the Post-Snowden Era* (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf 29
Qualcomm, *LTE Direct Proximity Services*, https://www.qualcomm.com/invention/technologies/lte/direct (last visited Sept. 25, 2017) 27

Miscellaneous—Continued: Page

Pamela Samuelson, *Privacy As Intellectual Property*, 52 Stan. L. Rev. 1125 (2000) 42

S. Rep. No. 541, 99th Cong., 2d Sess. (1986) 54

Tom Simonite, *Future Smartphones Won't Need Cell Towers to Connect*, MIT Tech. Review, Sept. 29, 2014, https://www.technologyreview.com/s/530996/future-smartphones-wont-need-cell-towers-to-connect/ 27

Sprint, *Sprint Corporation Privacy Policy* (Mar. 29, 2017), https://www.sprint.com/legal/privacy.html 3

T-Mobile, *T-Mobile Privacy Policy* (Dec. 31, 2016), https://www.t-mobile.com/company/website/privacypolicy.aspx#fullpolicy 4

Verizon, *Privacy Policy* (June 2017), http://www.verizon.com/about/privacy/full-privacy-policy 3

In the Supreme Court of the United States

No. 16-402

TIMOTHY IVORY CARPENTER, PETITIONER

v.

UNITED STATES OF AMERICA

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

BRIEF FOR THE UNITED STATES

OPINIONS BELOW

The opinion of the court of appeals (Pet. App. 1a-32a) is reported at 819 F.3d 880. The opinion and order of the district court denying petitioner's motion to suppress (Pet. App. 34a-48a) is not published in the Federal Supplement but is available at 2013 WL 6385838.

JURISDICTION

The judgment of the court of appeals was entered on April 13, 2016. A petition for rehearing was denied on June 29, 2016 (Pet. App. 33a). The petition for a writ of certiorari was filed on September 26, 2016. This Court's jurisdiction rests on 28 U.S.C. 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

Relevant provisions are reprinted in Appendix A, *infra*, 1a-12a.

STATEMENT

Following a jury trial in the United States District Court for the Eastern District of Michigan, petitioner was convicted on six counts of aiding and abetting Hobbs Act robbery, in violation of 18 U.S.C. 1951(a), and five counts of aiding and abetting the use or carrying of a firearm during and in relation to a crime of violence, in violation of 18 U.S.C. 924(c). Pet. App. 5a-6a. The district court sentenced petitioner to 1395 months in prison. *Id.* at 7a. The court of appeals affirmed. *Id.* at 1a-32a.

A. Cell-Site Records And The Stored Communications Act

1. Cellular telephones "work by establishing a radio connection with nearby cell towers (or 'cell sites')." Pet. App. 5a; see *id.* at 76a-77a. "[A] cell tower is a large antenna that emits a radio frequency" to cell phones within the tower's coverage area. J.A. 45. "[I]ndividual towers project different signals in each direction or 'sector,'" typically with three sectors per tower. Pet. App. 5a, 78a; J.A. 45. If a provider does not have towers covering a particular area, the provider may enter into a "roaming" agreement to use another provider's towers. J.A. 44; see J.A. 49-50, 63-64. In rural areas, "a tower's coverage might reach as far as 20 miles." Pet. App. 5a. "In an urban area like Detroit," where most of the robberies at issue occurred, "each cell site covers typically anywhere from a half-mile to two miles." *Ibid.* (internal quotation marks omitted).

When an individual places or receives a call on a cell phone, the phone scans its environment and connects to the cell site with the best signal, which will typically be the tower closest to the phone or in its direct line of sight. Pet. App. 76a-77a. Factors other than distance

may influence signal strength, including "buildings, topography," and "[t]he time of year." J.A. 48. During the call, the phone and tower transmit signals to each other to maintain the connection, and the phone may switch to a new tower if the signal strength fluctuates or the phone moves. J.A. 43-44, 83; Pet. App. 77a.

Cell-service providers "typically log and store certain call-detail records of their customers' calls, including the date, time, and length of each call; the phone numbers engaged on the call; and the cell sites where the call began and ended." Pet. App. 5a-6a. No law requires providers to create or maintain cell-site records; instead, providers retain those records in the ordinary course of business for their own purposes. *Id.* at 7a, 10a. Those purposes include finding weak spots in the providers' networks and applying roaming charges. *Ibid.* In addition, providers may sell aggregated cell-site data they collect or otherwise use that data in business ventures unrelated to providing cell-phone service. See, *e.g.*, Electronic Privacy Information Center (EPIC) Amicus Br. 22-23 (describing how cell-service providers sell location data to data brokers); Tech. Experts Amicus Br. 23 (stating that providers have "found commercial uses for location data"). Providers in the United States disclose their collection and use of cell-site data in their privacy policies.[1]

---

[1] See, *e.g.*, Verizon, *Privacy Policy* (June 2017), http://www.verizon.com/about/privacy/full-privacy-policy ("Verizon Wireless collects and uses mobile device location data for a variety of purposes."); AT&T, *AT&T Privacy Policy* (May 2, 2017), http://about.att.com/sites/privacy_policy/full_privacy_policy (explaining that AT&T collects and uses "[l]ocation information [that] is generated when [users'] device[s] communicate[] with cell towers"); Sprint, *Sprint Corporation Privacy Policy* (Mar. 29, 2017), https://www.sprint.com/legal/privacy.html (informing users that Sprint "may

2. The Stored Communications Act (SCA), 18 U.S.C. 2701 *et seq.*, authorizes the government to obtain cell-service providers' records pertaining to their subscribers under specified circumstances. 18 U.S.C. 2703. As relevant here, the government may require a provider "to disclose a record or other information pertaining to a subscriber * * * (not including the contents of communications)" through "a court order for such disclosure under [18 U.S.C. 2703(d)]." 18 U.S.C. 2703(c)(1)(B). To obtain a Section 2703(d) order, the government must "offer[] specific and articulable facts showing that there are reasonable grounds to believe that * * * the records or other information sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. 2703(d). On the provider's motion, the court "may quash or modify [a Section 2703(d)] order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden." *Ibid.* In addition, a provider may raise a Fourth Amendment challenge to a Section 2703(d) order, to ensure compliance with constitutional limits on the use of compulsory process. See *Donovan* v. *Lone Steer, Inc.*, 464 U.S. 408, 415 (1984) ("[T]he Fourth Amendment requires that [a] subpoena be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.") (citation omitted).

---

collect information about * * * [their] location" and use that information in a variety of circumstances); T-Mobile, *T-Mobile Privacy Policy* (Dec. 31, 2016), https://www.t-mobile.com/company/website/privacypolicy.aspx#fullpolicy (stating that T-Mobile's "systems capture details about the * * * location of wireless device[s] [customers] use").

B. The Present Controversy

1. Beginning in December 2010, petitioner and his co-conspirators committed a string of armed robberies at Radio Shack and T-Mobile stores in Ohio and Michigan. Pet. App. 3a, 6a. Petitioner typically organized the robberies, supplied the guns, and acted as a lookout. *Id.* at 5a. On petitioner's signal, a group of robbers "entered the store, brandished their guns, herded customers and employees to the back, and ordered the employees to fill the robbers' bags with new smartphones." *Ibid.* After each robbery, the team met nearby to dispose of the guns and getaway vehicle and sell the stolen merchandise. *Ibid.*

2. a. In April 2011, police arrested four of petitioner's co-conspirators, and one of them "confessed that the group had robbed nine different stores in Michigan and Ohio between December 2010 and March 2011, supported by a shifting ensemble of 15 other men who served as getaway drivers and lookouts." Pet. App. 3a. Based on that information, the government applied to federal magistrate judges for court orders pursuant to Section 2703(d) of the SCA. *Id.* at 3a-4a; see *id.* at 49a-55a, 62a-68a. As relevant here, those applications sought orders directing MetroPCS and Sprint to disclose non-content records for a cell-phone number that petitioner used, including "cell site information for [petitioner's] telephone[] at call origination and at call termination for incoming and outgoing calls." *Id.* at 4a. Specifically, the government requested 152 days of historical cell-site records from MetroPCS, spanning the period when the string of robberies occurred in Detroit between December 2010 and April 2011. *Id.* at 52a, 61a. The government sought seven days of records from Sprint, linked to the date of a robbery in Warren, Ohio,

where MetroPCS has a roaming agreement with Sprint. *Id.* at 65a, 80a.

The magistrate judges issued the requested orders. Pet. App. 4a; see *id.* at 56a-61a, 69a-73a. MetroPCS then produced 127 days of cell-site records and Sprint produced two days of records for petitioner's phone number. *Id.* at 7a; Pet. Br. 7. The records showed the towers petitioner's phone connected to when it made and received calls, but did not contain any cell-site information for text messages or for times when petitioner's phone was turned on but was not being used to connect a call. See Pet. App. 7a.

From the cell-site records, as well as MetroPCS and Sprint records identifying the locations of their towers, the government could infer the approximate location of petitioner's phone when calls were connected to it around the time of the robberies. Pet. App. 6a; J.A. 78-79. Because the cell sites covered areas "extending between one-half mile and two miles in length," however, the government could determine the location of petitioner's phone only "within a 3.5 million square-foot to 100 million square-foot area"—"as much as 12,500 times less accurate than * * * GPS data." Pet. App. 14a-15a. The government ultimately determined that petitioner's phone connected to cell towers in the general vicinity of the sites of four robberies around the times those robberies occurred. *Id.* at 6a.

b. Petitioner was indicted on six Hobbs Act counts and six firearms counts. Pet. App. 4a. Before trial, petitioner moved to suppress the cell-site records. *Id.* at 7a-8a. Petitioner argued that MetroPCS's and Sprint's production of their business records constituted a Fourth Amendment search of petitioner that could be

conducted only pursuant to a warrant supported by probable cause. *Ibid.*

The district court denied the motion to suppress. Pet. App. 34a-48a. The court found "no legitimate expectation of privacy in cell site data," *id.* at 38a, and further held that suppression would not be an appropriate remedy even if a warrant were required "because the agents relied in good faith on the [SCA] in obtaining the evidence," *id.* at 38a n.1.

c. The case proceeded to trial, where seven accomplices testified about petitioner's involvement in the robberies. Pet. App. 5a. The government also introduced videotapes and eyewitness testimony placing petitioner near the relevant robbery scenes. See Gov't C.A. Br. 45-47 (describing evidence).

In addition, FBI Special Agent Christopher Hess offered expert testimony about the cell-site data for petitioner's phone. Pet. App. 5a-6a; J.A. 36-129. Agent Hess explained that petitioner's providers recorded tower information only when the phone was "active," meaning "[e]ngaging in a call." J.A. 60; see J.A. 61 (testimony that "if you dial a number and you hit send, that tower information is populated in the call detail record," but records are not created when "the phone is just in [a] pocket" and not making or receiving calls). "The parties stipulate[d] and agree[d] that the telephone call detail records from * * * Metro PCS and Sprint" were "authentic and accurate business records of these companies." J.A. 51; see J.A. 136 (cell-site record for petitioner's phone on December 13, 2010).[2]

---

[2] This document is the only cell-site record for petitioner's phone in the record. Amici asked the court of appeals to take judicial notice of all the cell-site records MetroPCS produced, but the court declined, stating that it would not "create an evidentiary loophole

Based on those records, Agent Hess identified eight calls that occurred around the time of four robberies. Pet. App. 80a-82a; J.A. 56-67, 77-79. He presented maps of the towers that connected those calls to demonstrate that petitioner's phone was within a half-mile to two miles of the crime scenes. Pet. App. 6a, 86a-89a. But Agent Hess could not offer "any opinion about exactly where a phone was at any particular time" within each tower's coverage area. J.A. 88. He acknowledged that he could not determine from the cell-site records whether petitioner's phone was at a specific parking lot or intersection, J.A. 86-87; whether the phone was north or south of a store, J.A. 95; whether the phone had connected to a particular tower based on proximity or other "variables, such as * * * the battery strength," J.A. 84; "who was actually using the phone at the time that the call was made," J.A. 88; or why the phone was located within a particular tower's coverage area at a particular time, J.A. 95-96. Agent Hess acknowledged that his analysis of cell-site records was "not an exact science." J.A. 97-98.

The jury convicted petitioner on all the Hobbs Act counts and all but one of the firearms counts. Pet. App. 6a. The district court sentenced petitioner to 1395 months in prison. *Id.* at 7a.

3. The court of appeals affirmed. Pet. App. 1a-32a.

a. As relevant here, the court of appeals rejected petitioner's Fourth Amendment challenge, holding that

---

through which a litigant could present a district court with one record and then ask an appellate court to reverse the district court based on another record." Order 2 (Apr. 11, 2016).

the government's acquisition of the cell-site records was not a search of petitioner. Pet. App. 8a-17a.

The court of appeals emphasized that petitioner "lack[s] any property interest in cell-site records created and maintained by [his] wireless carriers." Pet. App. 12a. As the court explained, MetroPCS and Sprint gathered information about which of their towers connected petitioner's calls "in the ordinary course of business" for their own purposes, such as "to find weak spots in their network and to determine whether roaming charges apply." *Id.* at 10a.

The court of appeals further concluded that petitioner had no reasonable expectation of privacy in those business records. Pet. App. 7a-13a. The court relied on *Smith* v. *Maryland*, 442 U.S. 735 (1979), which "held that the police's installation of a pen register—a device that tracked the phone numbers a person dialed from his home phone—was not a search because the caller could not reasonably expect those numbers to remain private." Pet. App. 9a-10a. Because "Smith 'voluntarily conveyed numerical information to the telephone company and exposed that information to its equipment in the ordinary course of business,'" the "numerical information was not protected under the Fourth Amendment." *Id.* at 12a (internal quotation marks omitted) (quoting *Smith*, 442 U.S. at 744). The court of appeals concluded that the same reasoning applied to cell-site records because cell-phone users voluntarily convey information to their providers about their phones' proximity to particular towers "as a means of establishing communication" when they place or receive calls. *Ibid.* (quoting *Smith*, 442 U.S. at 741).

The court of appeals observed that "[w]hether a defendant ha[s] a legitimate expectation of privacy in certain information depends in part on what the government did to get it." Pet. App. 13a. Because "[t]his case involves business records obtained from a third party," the court found any expectation of privacy to be "diminish[ed]." *Id.* at 14a. The court further emphasized that the cell-site location data was "as much as 12,500 times less accurate" than GPS data and contained only "routing information" that "sa[id] nothing about the content of any calls." *Id.* at 10a, 14a.

The court of appeals noted that, in enacting the SCA, Congress "struck a balance" by requiring the government to "show 'reasonable grounds' but not 'probable cause' to obtain" cell-site records. Pet. App. 15a-16a (citation omitted). The court observed that "Congress is usually better equipped than courts are to answer the empirical questions that [new] technologies present." *Id.* at 17a. The court concluded that "[t]hese concerns favor leaving undisturbed the Congressional judgment" reflected by the SCA's "middle ground [approach] between full Fourth Amendment protection and no protection at all." *Id.* at 15a, 17a.[3]

b. Judge Stranch filed an opinion concurring in the judgment on the Fourth Amendment issue. Pet. App. 24a-32a. In her view, the government's acquisition of the historical cell-site records "raise[d] Fourth Amendment concerns," but the district court properly denied

---

[3] Because the court of appeals concluded that no search had occurred, it did not reach the government's alternative arguments that (i) any search was constitutionally reasonable, see Gov't C.A. Br. 37-40; (ii) the good-faith exception to the exclusionary rule applies, see *id.* at 40-42; and (iii) any error in admitting the cell-site data was harmless, see *id.* at 44-47.

the motion to suppress under the good-faith exception to the exclusionary rule. *Id.* at 24a-25a.

SUMMARY OF ARGUMENT

I. The government's acquisition of cell-site records from MetroPCS and Sprint did not constitute a Fourth Amendment search of petitioner.

A. Petitioner has no legitimate expectation of privacy in the business records his providers made of the cell towers used to route calls to and from his cell phone. This Court has long held that an individual cannot invoke the Fourth Amendment to object to the government's acquisition of a third party's records that contain information about the individual. See *Smith* v. *Maryland*, 442 U.S. 735 (1979) (records of dialed calls); *United States* v. *Miller*, 425 U.S. 435 (1976) (banking records).

The third-party doctrine applies here. Petitioner had no subjective expectation of privacy in his providers' records of the towers used to connect his calls. Cell-phone users are aware that they must be in a tower's coverage area to use their phones, and they must understand that their provider knows the location of its own equipment and may make records of the use of its towers. And any subjective expectation of privacy would not be objectively reasonable. Cell-phone users voluntarily reveal to their providers information about their proximity to cell towers so the providers can connect their calls. Users cannot reasonably expect that the providers will not reveal that business information to the government.

Contrary to petitioner's suggestion, cell-site records are not more sensitive than the records of phone numbers dialed and banking records at issue in *Smith* and *Miller*. Inferences about location drawn from cell-site

information are far less precise than GPS data and do not permit a detailed reconstruction of a person's movements. And in any event, the third-party doctrine does not turn on *what* information the government acquires and how sensitive that information is, but rather on *how* the government acquires the information. Seeking information about a suspect from a third-party witness does not amount to a Fourth Amendment search of that suspect, no matter how revealing or incriminating the evidence may be. Nor was petitioner's action in conveying information about his proximity to cell towers less "voluntary" than the defendants' actions in *Smith* and *Miller*. In those cases, like this one, individuals were required to reveal information about themselves to use an important service provided by a business that was a ubiquitous part of modern society.

Cell-service providers' use of technology does not justify a new Fourth Amendment rule. This case involves a traditional procedure used for centuries: compulsory process to a third party. The relevant change is not in government conduct, but in the actions of private providers in creating cell-tower networks and recording information about the networks' use. But a private actor's decision to acquire and record information is not a subject of Fourth Amendment protection.

Petitioner suggests that if the third-party doctrine is applied here, it would permit unregulated government collection of all information in a third party's hands, including email. That is incorrect. Email is routed through a provider, and its contents, like those of a sealed letter in the mail, may remain private. But cell-tower information is sent to the provider and used in its own business; it falls within the traditional third-party

doctrine. Moreover, adherence to the third-party doctrine does not eliminate all constitutional limitations on collection of data. Providers may invoke their own Fourth Amendment rights to object to compulsory process that exceeds legislative authorization, sweeps too broadly, or imposes undue burdens. The sensitivity of customer information may inform that calculus. The First Amendment and equal protection principles also protect against abuses. And if businesses' possession of great quantities of digital information raises new privacy concerns, legislatures are well positioned to address them.

B. Petitioner was not subject to a trespassory search under *United States* v. *Jones*, 565 U.S. 400 (2012). He can establish no protected interest in the providers' cell-tower records, and his reliance on positive law to claim such an interest lacks merit.

II. If the government's acquisition of cell-site records amounted to a search of petitioner, it was constitutionally reasonable.

A. Under longstanding Fourth Amendment principles, the government's use of compulsory process to obtain records does not require a warrant. Section 2703(d) falls within that tradition and in fact raises the bar from a subpoena by requiring a specific factual showing and a court order, thereby adequately protecting any expectation of privacy a customer could assert in cell-site records.

B. Applying standard Fourth Amendment balancing principles leads to the same conclusion. Any privacy interest in third-party business records is diminished. And the government has a compelling interest in obtaining cell-site records to identify suspects, clear the inno-

cent, and obtain information in the preliminary investigation of criminal conduct. Deference to Congress's judgment in Section 2703(d) is appropriate in this new technological context.

III. If the Court concludes that a warrant is required to obtain some cell-site records, it should hold, as petitioner concedes, that requests for short-term cell-site records fall outside that rule. Here, that principle would validate the request for seven days of records from Sprint, as that is well within the range of ordinary visual surveillance of a person suspected of a crime.

ARGUMENT

I. THE GOVERNMENT'S ACQUISITION OF PROVIDERS' BUSINESS RECORDS OF THE TOWERS USED TO CONNECT PETITIONER'S CALLS DID NOT CONSTITUTE A FOURTH AMENDMENT SEARCH OF PETITIONER

The Fourth Amendment provides in relevant part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. Amend. IV. An individual may claim protection against a Fourth Amendment "search" in two circumstances. First, he may establish that he has been searched if "the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo* v. *United States*, 533 U.S. 27, 33 (2001); see *Katz* v. *United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Second, he may establish that he has been searched if he is subject to a "physical intrusion of a constitutionally protected area," in a manner that would constitute a "common-law trespass." *United States* v. *Jones*, 565 U.S. 400, 405, 407 (2012) (citation omitted). Under either approach, the government's acquisition of

MetroPCS's and Sprint's business records of the cell towers used to connect petitioner's calls did not constitute a Fourth Amendment search of petitioner.

A. A Cell-Phone User Has No Reasonable Expectation Of Privacy In Business Records Created By His Provider Documenting The Cell Sites Used To Connect His Calls

1. Petitioner cannot claim a legitimate privacy interest in information about his proximity to cell towers that he disclosed to his cell-service providers

a. "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith* v. *Maryland*, 442 U.S. 735, 743-744 (1979). Third-party service providers who receive such information are free to create business records pertaining to the service they provide to their customers. *Id.* at 745. And the Court has held that the government's subsequent acquisition of those records does not constitute a Fourth Amendment search of the customer. See *id.* at 744-745; *United States* v. *Miller*, 425 U.S. 435, 442-443 (1976).

In *Miller*, the government subpoenaed a defendant's banks for several months of records of his accounts, including copies of his checks, deposit slips, financial statements, and monthly statements. 425 U.S. at 436-438. The defendant contended that he had "a reasonable expectation of privacy" in those records because "they [were] merely copies of personal records that were made available to the banks for a limited purpose." *Id.* at 442. But the Court rejected that argument, observing that it had "held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him

to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose." *Id.* at 443. The Court explained that the defendant could "assert neither ownership nor possession" of the records; rather, they were "business records of the banks." *Id.* at 440. Because those records "contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," the Court concluded that the defendant had "take[n] the risk, in revealing his affairs to another, that the information w[ould] be conveyed by that person to the Government." *Id.* at 442, 443.

In *Smith*, the Court applied the same principles to information conveyed to a telephone company. There, the police requested that the defendant's telephone company install a pen register at its offices to record the numbers dialed from the defendant's home phone. 442 U.S. at 737. The Court rejected the defendant's argument that the government's acquisition of the records of his dialed numbers qualified as a Fourth Amendment search. *Id.* at 742-746.

Smith first expressed "doubt that people in general entertain any actual expectation of privacy in the numbers they dial," given that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." 442 U.S. at 742. The Court believed that the typical user would be aware that the phone company could choose to record the numbers he dialed and would "in fact record this information for a variety of legitimate business purposes." *Id.* at 743. "Most phone books," the Court observed, inform users "that the [phone] company can frequently help in identifying to the authorities the origin

of unwelcome and troublesome calls." *Id.* at 742-743 (internal quotation marks omitted).

Smith went on to explain that "even if [the defendant] did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable." 442 U.S. at 743 (citation and internal quotation marks omitted). "When [the defendant] used his phone," the Court observed, he "voluntarily conveyed numerical information to the telephone company and exposed that information to its equipment in the ordinary course of business." *Id.* at 744 (internal quotation marks omitted). Because the company was "free to record" the information the defendant conveyed about the numbers he was dialing, the Court concluded that he "assumed the risk" that the company's records "would be divulged to police." *Id.* at 745.

The Court's recognition that individuals cannot claim a reasonable expectation of privacy vis-à-vis the government in information they disclose to third parties has deep historical roots. It is an "ancient proposition of law" that "'the public . . . has a right to every man's evidence,' except for those persons protected by a constitutional, common-law, or statutory privilege." *United States* v. *Nixon*, 418 U.S. 683, 709 (1974) (citation omitted). "[A]s early as 1612, * * * Lord Bacon is reported to have declared that 'all subjects, without distinction of degrees, owe to the King tribute and service, not only of their deed and hand, but of their knowledge and discovery.'" *Blair* v. *United States*, 250 U.S. 273, 279-280 (1919) (quoting *Countess of Shrewsbury Case*, 2 How. St. Tr. 769, 778 (1612)). As this Court has recognized, "[t]o ensure that justice is done, it is imperative to the function of courts that compulsory process be

available for the production of evidence." *Nixon*, 418 U.S. at 709.

A witness who observes relevant events must therefore testify about them when asked to do so, unless a recognized privilege applies. A desire for privacy does not trigger a privilege, as no "constitutional provision protects the average citizen from disclosing * * * information that he has received in confidence." *Branzburg* v. *Hayes*, 408 U.S. 665, 682 (1972). Accordingly, a person who "rel[ies] upon his misplaced confidence that [a third party] w[ill] not reveal his wrongdoing" cannot claim a legitimate expectation that the information will remain private. *Hoffa* v. *United States*, 385 U.S. 293, 302 (1966). He therefore cannot invoke the Fourth Amendment to prevent the government from obtaining the third party's testimony, evidence, or records that reveal matters he has disclosed. *SEC* v. *Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984).

b. The Court's third-party cases establish that petitioner has no Fourth Amendment interest in MetroPCS's and Sprint's records of the cell towers they used to connect his calls.

i. Petitioner lacks any subjective expectation of privacy in the cell-site information because his providers compiled that data based on their transactions with petitioner for their own business purposes. See Pet. App. 7a, 10a. As with the bank records in *Miller*, petitioner "can assert neither ownership nor possession" of the cell-site records, 425 U.S. at 440; indeed, he "stipulate[d] and agree[d]" that they were "business records of [MetroPCS and Sprint]." J.A. 51. "Although subjective expectations cannot be scientifically gauged," cellphone users, like landline users, should not be pre-

sumed to have a "general expectation" that data generated by their use of telephone-company equipment and incorporated into the company's records "will remain secret." *Smith*, 442 U.S. at 743.

Petitioner contends (Br. 42-44) that cell-phone users may not realize the extent of the information they disclose about their location when they use their providers' towers to connect their calls. But as petitioner recognizes (Br. 42-43), cell-phone users surely "have a general sense that their cell phones must communicate with the service provider's cell towers in order to place and receive calls." "[A]ny cellphone user who has seen her phone's signal strength fluctuate must know that, when she places or receives a call, her phone 'exposes' its location to the nearest cell tower and thus to the company that operates the tower." Pet. App. 12a; see, *e.g.*, *United States* v. *Graham*, 824 F.3d 421, 430 (4th Cir. 2016) (en banc), petitions for cert. pending, Nos. 16-6308 and 16-6694 (filed Sept. 26 and Oct. 27, 2016); *United States* v. *Davis*, 785 F.3d 498, 511 (11th Cir.) (en banc), cert. denied, 136 S. Ct. 479 (2015); *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 613 (5th Cir. 2013) (*Fifth Circuit In re Application*); see also *Smith*, 442 U.S. at 743 (relying on what telephone users "typically know" to refute any subjective expectation of privacy). If any doubt existed on that point, "contractual terms of service and providers' privacy policies expressly state that a provider uses a subscriber's location information to route his cell phone calls." *Fifth Circuit In re Application*, 724 F.3d at 613; see p. 3 n.1, *supra* (citing policies); see also *Smith*, 442 U.S. at 742-743 (finding no subjective privacy expectation in dialed numbers in part because "[m]ost phone

books t[old] subscribers" that the phone company could help identify the source of unwelcome calls).[4]

Petitioner further errs in asserting (Br. 43) that cell-phone users may subjectively expect that routing information for their calls will remain private because they "do not receive their [cell-site location information] in their monthly bill" and "cannot know whether the service provider is logging and retaining that data and in what form or detail." The *Smith* Court rejected similar arguments. There, the Court acknowledged that "most people may be oblivious to a pen register's esoteric functions," 442 U.S. at 742, and that telephone users would not ordinarily see lists of the local numbers they dialed because "telephone companies, in view of their present billing practices, usually do not record local calls," *id.* at 745. But the Court nevertheless found that users are generally aware that companies can track the numbers dialed and are "free to record" that information. *Ibid.* Cell-phone users similarly should be charged with knowledge "that they must transmit signals to cell towers within range, that the cell tower functions as the equipment that connects the calls, that users when making or receiving calls are necessarily con-

---

[4] Petitioner notes (Br. 42) that some smart phones "have a location privacy setting that, when enabled, prevents applications" from using GPS data to access a phone's location. Petitioner speculates that users who enable that feature may incorrectly think they are preventing their providers from collecting cell-site data. Any such misconception contradicts the providers' privacy policies and users' understanding that their phones must connect to cell towers to work. And if a cell-phone user elected *not* to enable the privacy setting, that conduct would simply confirm that the user lacked a subjective expectation of privacy in the data her provider collects.

veying or exposing to their service provider their general location within that cell tower's range, and that cell phone companies make records of cell-tower usage" or are free to do so. *Davis*, 785 F.3d at 511.

ii. In any event, any subjective expectation of privacy in information a user conveys to his provider about his proximity to cell towers would not be objectively reasonable because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743-744. Just as a person who dials a phone number "voluntarily convey[s] numerical information to the telephone company and expose[s] that information to its equipment in the ordinary course of business," *id.* at 744 (internal quotation marks omitted), a cell-phone user reveals general information about his location to his provider so that it can connect his calls. A cell-phone user thus has no valid basis for complaint if the provider makes use of that business information, including by providing it to the government. See *Miller*, 425 U.S. at 443.

Petitioner contends (Br. 21) that his asserted expectation of privacy is reasonable based on "protections adopted in federal and state law." Petitioner relies (Br. 21-22) on 47 U.S.C. 222, which generally prohibits cell-service providers from using or disclosing certain information, including cell-site information and records of the numbers a customer has dialed. 47 U.S.C. 222(c)(1), (d), and (h)(1). But the statute enumerates several exceptions to that general rule and further permits disclosure "as required by law," 47 U.S.C. 222(c)(1)—which includes a valid court order

issued pursuant to the SCA.[5] A cell-phone user consulting federal law therefore could not reasonably believe that Section 222 prevents the government from obtaining providers' cell-site records. Nor could this Court credit such a belief without overruling *Smith*'s holding that users have no reasonable expectation of privacy in the phone numbers they dial—a category of information also protected by Section 222. See 47 U.S.C. 222(h)(1).

Petitioner's reliance on Section 222 is also wrong as a matter of Fourth Amendment jurisprudence. Although statutes "enacted in the years immediately before or after the [Fourth] Amendment was adopted shed light on what citizens at the time of the Amendment's enactment saw as reasonable," the Court has rejected the suggestion that "the Amendment was intended to incorporate subsequently enacted statutes." *Virginia* v. *Moore*, 553 U.S. 164, 169 & n.3 (2008). Congress can enact statutory privacy protections that go beyond the Fourth Amendment floor—and it has restricted disclosure of a variety of third-party records pertaining to individuals who cannot claim Fourth Amendment protection of those records. See, *e.g.*, 15 U.S.C. 6802 (financial records); 26 U.S.C. 7216 (information used to prepare tax returns). But "no historical indication [exists] that those who ratified the Fourth Amendment understood it as a redundant guarantee of" statutory protections. *Moore*, 553 U.S. at 168.

---

[5] Petitioner notes (Br. 22) that Section 222 requires providers to obtain a user's "express prior authorization" before disclosing location data based on the user's consent. 47 U.S.C. 222(f). But that rule for establishing consent does not displace the many other provisions permitting disclosure *without* the user's approval, including "as required by law." 47 U.S.C. 222(c)(1).

Petitioner's reliance on state law (Br. 22-23) is similarly misplaced. Some States have required a search warrant for historical cell-site records as a matter of state law, but this Court has repeatedly rejected the "suggestion that concepts of privacy under the laws of each State are to determine the reach of the Fourth Amendment." *California* v. *Greenwood*, 486 U.S. 35, 44 (1988). Rather, "when States go above the Fourth Amendment minimum, the Constitution's protections concerning search and seizure remain the same." *Moore*, 553 U.S. at 173. The enactment of state laws addressing cell-site records confirms that legislatures are best positioned to balance privacy interests and law-enforcement needs in light of new technologies, as Congress did in the SCA. See *Jones*, 565 U.S. at 429-430 (Alito, J., concurring in the judgment). But state laws do "not alter the content of the Fourth Amendment" and so cannot help petitioner establish that the government's acquisition of his cell-service providers' business records constituted a Fourth Amendment search of him. *Moore*, 553 U.S. at 172.

2. Petitioner cannot distinguish this Court's cases finding no reasonable expectation of privacy in information conveyed to a third party

Petitioner argues (Br. 35-47) that the third-party doctrine should not apply to longer-term cell-site records, but his attempts to distinguish *Smith* and *Miller* lack merit.

a. Petitioner asserts (Br. 36) that "[t]he particular records at issue here are far more sensitive and personal than those in *Smith* and *Miller*." That contention is both factually inaccurate and legally irrelevant.

i. Petitioner stakes his asserted expectation of privacy on his claim (Br. 3) that the government's acquisition of cell-site information "make[s] it possible to reconstruct in detail everywhere an individual has traveled over hours, days, weeks, or months." That is incorrect. Although petitioner likens cell-site records to GPS tracking, cell-site location information is actually "as much as 12,500 times less accurate" than GPS data. Pet. App. 14a. Rather than pinpoint petitioner's precise location, the records identified "a 3.5 million square-foot to 100 million square-foot area," *ibid.*—an area that would cover about 180 to 5155 oval plazas equal in size to the one in front of the Supreme Court building. See *Hodge* v. *Talkin*, 799 F.3d 1145, 1151 (D.C. Cir. 2015) (providing measurements of the Court's plaza), cert. denied, 136 S. Ct. 2009 (2016). When such an area encompasses a crime scene, cell-site records may be consistent with the government's theory that a defendant was there, but they do not on their own suffice to place him at the crime scene. See Pet. App. 89a. The government must instead rely on reasonable inferences or additional evidence—*e.g.*, eyewitness accounts and video surveillance like that introduced at petitioner's trial—to develop proof of a defendant's movements.

The cell-site records in this case illustrate the point. On December 13, 2010, for example, petitioner's phone connected to two cell towers close in time to the robbery of a Radio Shack in Detroit. Pet. App. 86a. During the first call, petitioner's phone connected to a tower more than a dozen blocks southwest of the Radio Shack, and during the second call, petitioner's phone initially connected to a tower at least eight blocks northeast of the store. *Ibid.* An excerpt of the map Agent Hess created shows that area:

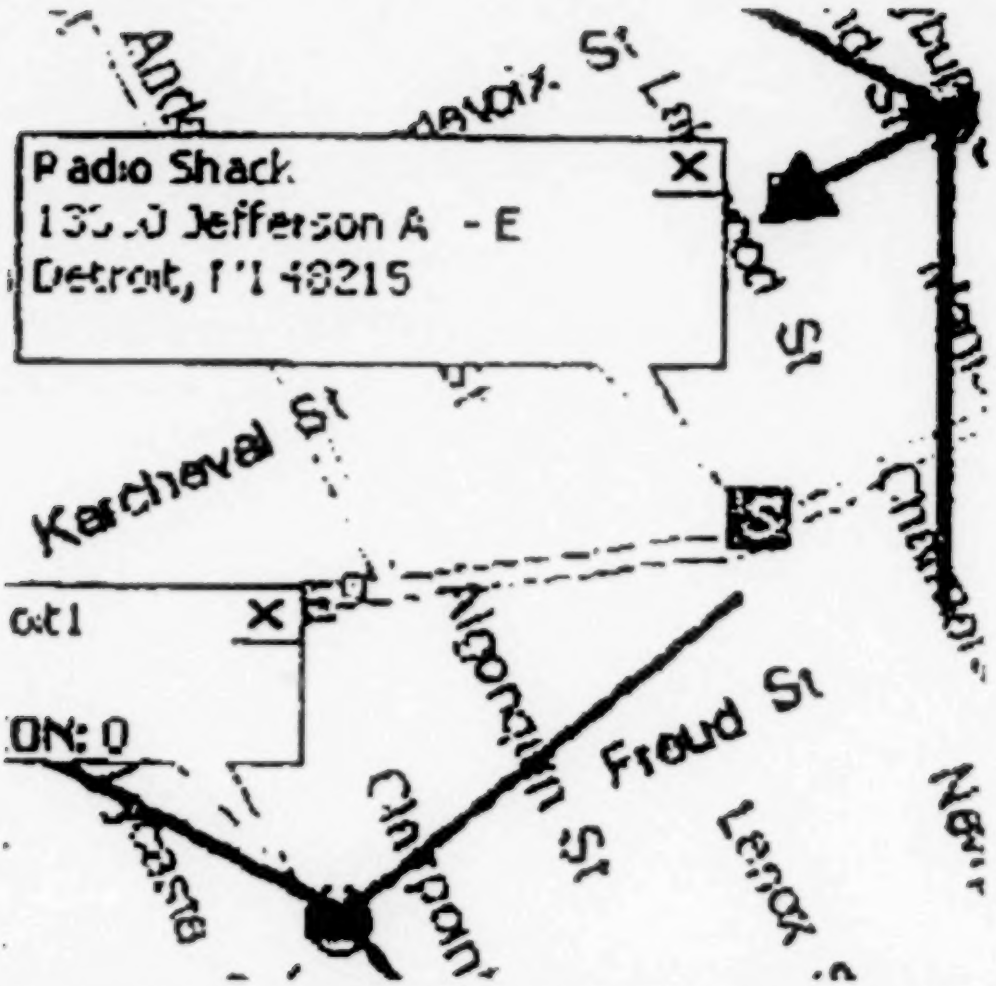


Figure 1 – Excerpt from Gov't Ex. 57 (Pet. App. 86a)

As reflected in the following illustration using data from Google Maps, the area approximately within the relevant tower sectors today contains about 1000 buildings, including hundreds of homes, various commercial establishments, more than one dozen houses of worship, several civic buildings, numerous multi-unit apartment buildings, and a large automobile assembly plant.[6]

---

[6] Appendix B, *infra*, 13a, explains the methodology used to create Figure 2, which is not in the record and is offered to illustrate the approximate density and variety of buildings in the area given petitioner's assertion (Br. 17) that cell-site records reveal religious preferences, doctor's visits, shopping habits, or other places visited.

Figure 2 – Illustrative map of buildings in the area

While the cell-site data corroborated other evidence of petitioner's participation in the December 13 robbery, it could not reveal the exact whereabouts of his phone within the towers' coverage area. J.A. 88, 131-132. From the records alone, the government could not determine whether petitioner (or someone using his phone) was at the Radio Shack, or instead at any one of the nearby bars, restaurants, stores, schools, banks, gas stations, other commercial establishments, or homes.

Petitioner contends (Br. 27-29) that cell-site records will enable more precise inferences about an individual's location in the future as providers deploy cell towers with smaller coverage areas. But petitioner identifies no case in which the government has obtained records involving small-cell technology. And the technology could develop in a different direction. For example, device-to-device technology could reduce the need for cell towers, preventing providers from collecting or recording location information. See, *e.g.*, Tom Simonite, *Future Smartphones Won't Need Cell Towers to Connect*, MIT Tech. Review, Sept. 29, 2014, https://www.technologyreview.com/s/530996/future-smartphones-wont-need-cell-towers-to-connect/ (describing technology); Qualcomm, *LTE Direct Proximity Services*, https://www.qualcomm.com/invention/technologies/lte/direct (last visited Sept. 25, 2017) (asserting that device-to-device technology protects location privacy because it "allow[s] the devices to discover others without revealing their own identity or exact location"). Similarly, all major cell-service providers now offer built-in wi-fi calling, which may reduce providers' access to "network location information." Lennart Norell et al., *Wi-Fi calling —extending the reach of VoLTE to Wi-Fi*, Ericsson Review 1, 3-5 (Jan. 30, 2015), https://www.ericsson.com/

res/thecompany/docs/publications/ericsson_review/2015/er-wifi-calling.pdf. Because the Court "risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear," it should decline petitioner's invitation to consider the Fourth Amendment's application in hypothetical circumstances not presented by the facts of his case. *City of Ontario* v. *Quon*, 560 U.S. 746, 759 (2010).

ii. In any event, petitioner errs in suggesting that the sensitivity of information in a third party's records triggers a reasonable expectation of privacy in those records.[7] The application of the third-party doctrine does not depend on the quantity of information disclosed to the third party or on how revealing or incriminating that information may be. Records of the telephone numbers a person dials may reveal intensely personal information about her associations. See *Smith*, 442 U.S. at 748 (Stewart, J., dissenting) (observing that such records "easily could reveal the identities of the persons and the places called, and thus

---

[7] Petitioner cites (Br. 37) *Ferguson* v. *City of Charleston*, 532 U.S. 67 (2001), and *Stoner* v. *California*, 376 U.S. 483 (1964), but those cases did not address whether the government conducts a search of an individual by acquiring information about him that he has conveyed to a third party. *Ferguson* involved urine tests that "were indisputably [Fourth Amendment] searches," 532 U.S. at 76, and the only question was whether "special needs" allowed government actors to conduct the tests and share the results with nonmedical personnel, *id.* at 77-81. *Stoner* involved a Fourth Amendment search of a hotel room, and the only question was whether the clerk who unlocked the door for the officers had authority to consent to the search. 376 U.S. at 485-488.

reveal the most intimate details of a person's life").[8] Records detailing every banking transaction an individual conducts likewise may contain sensitive information about her finances, spending habits, and financial relationships. *Miller*, 425 U.S. at 451 (Brennan, J., dissenting) (observing that "the totality of bank records provides a virtual current biography" because "[i]n the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations") (citation omitted). Despite the sensitivity of that information, this Court has recognized that disclosure to a third party vitiates a reasonable expectation that the information will remain private, "even if [it] is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* at 443 (majority opinion). Accepting petitioner's argument about sensitive third-party records would not provide a way to distinguish *Smith* and *Miller*, but would instead represent a stark departure from their rationales.

Petitioner's contention (Br. 37-38) that "the 'third party' doctrine * * * can be overcome when highly sensitive information is at stake" would also generate intractable line-drawing problems. Petitioner suggests no framework for determining when information conveyed to a third party should be considered sufficiently

---

[8] Empirical studies have established that "a similar number of adults regard the phone numbers they call to be just as 'sensitive' as location data." *United States* v. *Graham*, 796 F.3d 332, 382 n.5 (4th Cir. 2015) (Motz, J., dissenting in part and concurring in the judgment) (citing Pew Research Ctr., *Public Perceptions of Privacy and Security in the Post-Snowden Era* 34-35 (Nov. 12 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf), rev'd en banc, 824 F.3d 421 (4th Cir. 2016).

sensitive that it gives rise to a Fourth Amendment interest. And investigators cannot reasonably apply the standard to determine which third-party record requests require a warrant because they cannot know the particular contents of the records or the quantity of information they contain in advance. See *Atwater* v. *City of Lago Vista*, 532 U.S. 318, 347 (2001) (observing that "a responsible Fourth Amendment balance is not well served by standards requiring sensitive, case-by-case determinations * * * lest every discretionary judgment in the field be converted into an occasion for constitutional review").

Petitioner's proposed revision of the third-party doctrine is unworkable even as applied to location information. Petitioner concedes (Br. 29-31) that individuals have no reasonable expectation of privacy in records that reveal some amount of location data. But he declines to suggest how much is too much. And it is not evident when his rule would bar investigators from accessing a variety of records that may reveal information about a person's location or movements—from credit-card records that identify the places and times he made purchases, to IP-address records that reveal when he used a computer in a particular location, to pen-register records that show when he made calls from his home telephone, to key-card-entry records that reflect his regular hours at a gym. The practical problems posed by petitioner's argument counsel against his innovative suggestion that individuals may claim a Fourth Amendment interest in the records of their transactions with businesses from which their location can be inferred.

b. Petitioner further seeks to distinguish *Miller* and *Smith* (Br. 39-44) by contending that cell-phone users

do not voluntarily convey information about their location to their providers. Petitioner emphasizes (Br. 39) the importance of cell-phone use in modern society and argues that "[t]he act of possessing a cell phone, and even more so the transmission of location information, is not voluntary in any meaningful way."

Petitioner's argument misunderstands the circumstances under which this Court has applied the third-party doctrine. An individual who shares information about himself in the course of obtaining a third party's services need not necessarily be happy to expose those private details of his life to the business. Indeed, he may feel as though he has no choice if he wishes to use the third party's services. The depositor in *Miller*, for example, may not have relished sharing his financial affairs with his bank, as necessary to conduct banking transactions. See 425 U.S. at 451 (Brennan, J., dissenting) (observing that the depositor's actions were "not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account"). The telephone user in *Smith* likewise had no choice but to communicate the numbers he dialed to his telephone company, unless he was "prepared to forgo use of what for many has become a personal or professional necessity." 442 U.S. at 750 (Marshall, J., dissenting). But this Court nevertheless found that the individuals in *Smith* and *Miller* had "voluntarily conveyed" information about themselves to third parties—even though they had no ability to avoid exposing the information short of discontinuing use of the third party's services. *Smith*, 442 U.S. at 744; *Miller*, 425 U.S. at 442.

Petitioner accordingly cannot avoid application of the third-party doctrine by observing (Br. 39) that cell

phones are "a pervasive and insistent part of daily life." *Riley* v. *California*, 134 S. Ct. 2473, 2484 (2014). An individual's decision to expose his proximity to cell towers to his cell-service provider so it can connect his calls is just as volitional as his action in exposing the numbers he dials to that provider for the same purpose—and petitioner accordingly has not offered a tenable way to distinguish *Smith* and *Miller*.

3. Cell-service providers' use of technology supplies no basis to depart from well-established Fourth Amendment principles

Petitioner contends (Br. 10-11) that the Court should exempt cell-site records from the third-party doctrine because cell-service providers used technology to collect "a great volume" of information about him that the government could not have obtained "prior to the digital age." The Court should reject that argument.

1. In analyzing whether a Fourth Amendment search has occurred "it is important to begin by specifying precisely the nature of the state activity that is challenged." *Smith*, 442 U.S. at 741; see *Jones*, 565 U.S. at 404 ("It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information."). This Court's focus on the character of the government's conduct reflects that the existence of a Fourth Amendment search turns on *how*—not just *whether*—information is obtained. For example, "[a] phone conversation is private when overheard by means of a wiretap; but that same conversation is unprotected if an agent is forced to overhear it while seated on a Delta flight." Pet. App. 13a. "Similarly, information that is not particularly sensitive—say, the color of a suspect's vehicle—might be protected if government

agents broke into the suspect's garage to get it," but "information that is highly sensitive—say, all of a suspect's credit-charges over a three-month period—is not protected if the government gets that information through business records obtained per a subpoena." *Ibid.*

The government here obtained a third party's business records pursuant to a court order authorized by law. The character of the government's conduct fundamentally distinguishes this case from those in which the Court has expressed concern about the potential of new technology to erode privacy. Petitioner cites (Br. 15) *Jones*, *supra*, and *Kyllo*, *supra*, but in those cases government agents used technology to enhance their surveillance of a suspect.[9] In *Jones*, the government surreptitiously installed a GPS tracking device on a vehicle to monitor its movements for 28 days. 565 U.S. at 402-403. And in *Kyllo*, the government used a thermal imaging device that was "not in general public use[] to explore details of the home that would previously have been unknowable without physical intrusion." 533 U.S. at 40. In both cases, this Court held that the

---

[9] Petitioner also cites (Br. 15) *Riley*, *supra*, which held that officers generally must obtain a warrant before "search[ing] digital information on a cell phone seized from" an arrestee. 134 S. Ct. at 2480. But the government action in *Riley* indisputably constituted a Fourth Amendment search, and the only question was whether that search fell within the traditional search-incident-to-arrest exception to the warrant requirement. See *id.* at 2482. The analysis in *Riley* sheds no light on whether the qualitatively different government action of seeking evidence from a third party is a search in the first place. See *id.* at 2489 n.1 (explaining that the case did "not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances").

government's conduct constituted a search—a result that the Court concluded would "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Jones*, 565 U.S. at 406 (brackets in original) (quoting *Kyllo*, 533 U.S. at 34). But the Court's analysis in both cases made clear that the Fourth Amendment protects against particular *means* of acquiring information—not against the end results of that action. See *id.* at 408 n.5 ("[T]he obtaining of information is not alone a search unless it is achieved by * * * a trespass or invasion of privacy."); *Kyllo*, 533 U.S. at 35 n.2 ("The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment.").

Far from "employ[ing] new technology" in this case, Pet. Br. 10, the government used a method of obtaining evidence that was in use at least two hundred years before adoption of the Fourth Amendment: compulsory process to witnesses. See *Blair*, 250 U.S. at 279-280 (describing history of compulsory process dating to 1562). "[T]he general common-law principle that 'the public has a right to every man's evidence' was considered an 'indubitable certainty' that 'c[ould not] be denied' by 1742." *Kastigar* v. *United States*, 406 U.S. 441, 443 (1972). "[G]uidance from the founding era," *Riley*, 134 S. Ct. at 2484, therefore confirms that the government's conduct in seeking information about an individual from a third party has never been understood to constitute a Fourth Amendment search of that individual.

2. Petitioner's technology-based argument accordingly must focus on the actions of his *cell-service providers* in collecting and recording information about which towers they used to connect his calls. Even if that

conduct intruded on petitioner's privacy interests, however, the Fourth Amendment does not protect him from that private action. See *United States* v. *Jacobsen*, 466 U.S. 109, 113 (1984) (Fourth Amendment "proscrib[es] only governmental action"). And the government's later acquisition of the providers' business records likewise cannot be characterized as a Fourth Amendment search of petitioner because the government did not "exceed[] the scope" of any intrusion by the providers. *Id.* at 115.

The Court applied those principles to reject a Fourth Amendment challenge in *Jacobsen*. There, employees of a common carrier opened a damaged cardboard box and saw drugs inside. 466 U.S. at 111. They notified federal agents, who reopened the box and found the drugs. *Id.* at 111-112. This Court concluded that the agents' action "infringed no legitimate expectation of privacy and hence was not a 'search' within the meaning of the Fourth Amendment." *Id.* at 120. That result "follow[ed] from the analysis applicable when private parties reveal other kinds of private information to the authorities." *Id.* at 117 (citing, *inter alia*, *Miller*, 425 U.S. at 443, and *Smith*, 442 U.S. at 743-744). "Once frustration of the original expectation of privacy occurs" through a third party's action, the Court explained, "the Fourth Amendment does not prohibit governmental use of the now nonprivate information." *Ibid.* Accordingly, the "Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." *Ibid.*

To the extent the cell-service providers intruded on petitioner's privacy interests by recording which towers they used to route his calls, the government played no

role in that conduct. Petitioner's providers created and maintained those cell-site records for their own business purposes. See Pet. App. 10a. They chose when to collect tower information and how long to retain those records. Indeed, the government has far less to do with the record collection here than in *Miller*, where federal law mandated that banks keep records of banking transactions. 425 U.S. at 443. Here, the cell-service providers not only decided what cell-site records to keep, but whether and when to use the data they collected for commercial purposes. See p. 3, *supra*. Because the government's acquisition of the providers' records did not reveal any information that the providers had not already themselves obtained, the Fourth Amendment does not protect against disclosure of the cell-site information.

3. Petitioner contends (Br. 44-47) that applying the third-party doctrine to cell-site records will permit unregulated government acquisition of all digital information in a third party's possession, including email content. That argument ignores the distinction between information conveyed to the provider and information conveyed to others that the provider merely carries, transports, or stores. Moreover, the government faces various limitations on its ability to collect data from third parties, and policymakers can enact additional privacy protections if society deems them warranted.

a. Application of the third-party doctrine here does not mean (Pet. Br. 45) that "people would have no reasonable expectation of privacy even in their emails, because the contents of those communications are shared with a third party." The Court has made clear that in-

dividuals who rely on a third party to deliver their communications do not thereby lose an expectation of privacy in the contents of those communications. See *Ex parte Jackson*, 96 U.S. 727, 733 (1878). Thus, a person who mails a private letter retains a legitimate expectation of privacy in its contents, even though the letter travels through the hands of postal carriers en route to its destination. *Ibid.* At the same time, no privacy expectation exists in the routing information conveyed to the carriers to facilitate the delivery. See *ibid.* The differential treatment of those categories of information turns on whether the information has been communicated *to* the providers or merely passes *through* their communications networks, with no general right of the provider to use or control the contents. From the providers' point of view, "the content of personal communications is private" but "the information necessary to get those communications from point A to point B is not." Pet. App. 9a.

Petitioner is therefore wrong to assert (Br. 47) that "there is no way to distinguish emails" from cell-site records. Cell-phone users do not convey the content of their emails, calls, and text messages to their cell-service providers for the providers' unrestricted use. But the users do convey information to their providers about the users' proximity to particular cell towers to enable the routing of those emails, calls, and text messages. Applying the third-party doctrine to business records that providers create from that routing information, which pertain to the customers' use of the providers' towers, accordingly would not undermine

Fourth Amendment protection for the content of those private communications.[10]

b. Petitioner states (Br. 46) that individuals today disclose a "vast array of information" about themselves to third parties when using those parties' services. See also *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). Third parties' business records thus may contain increased quantities of information, as individuals choose to disclose that information to obtain desired services. But the character of the government's conduct—using compulsory process to obtain those records—has not changed. That conduct therefore is still not a Fourth Amendment search of the customer.

Petitioner expresses concern (Br. 14) that applying the third-party doctrine to records of his tower connections will leave all such data beyond constitutional control, making it possible for the government to collect all Americans' cell-site data for all time. That is incorrect. Providers have Fourth Amendment rights and may enforce well-established limits on the government's ability to request their business records, including protections

---

[10] Courts have recognized that the Fourth Amendment may protect the content of communications routed through a third-party provider even when the provider retains a limited right of access. See, *e.g.*, *United States* v. *Warshak*, 631 F.3d 266, 287 (6th Cir. 2010) (observing that "at the time *Katz* was decided, telephone companies had a right to monitor calls in certain situations"). Such incidental access does not undermine the principle that "the contents of letters, phone calls, and emails, which are not directed to a business, but simply sent via that business, are generally protected." *Fifth Circuit In re Application*, 724 F.3d at 611. Cell-site records, however, are not protected because they "are the providers' own records of transactions to which it is a party" and contain only information that is conveyed to providers so that they can route their customers' calls. *Id.* at 612.

against arbitrariness, overbreadth, and burdensomeness. See pp. 44-45, *infra*. That framework, enforceable through pre-compliance judicial review, can protect against "dragnet" collection efforts (Pet. Br. 45), even though individual customers cannot claim to have been searched. Cf. *United States* v. *Knotts*, 460 U.S. 276, 283-284 (1983) (reserving judgment on whether the Fourth Amendment may apply differently to "dragnet-type law enforcement practices"). The use of compulsory process also requires legislative authorization, see p. 44, *infra*, thus ensuring democratic accountability and legislative balancing of societal needs and individual interests, as appropriate for emerging technologies.

Limitations other than the Fourth Amendment also apply. The First Amendment regulates acquisition or use of information to suppress free speech or association, and equal protection principles protect against "intentionally discriminatory application of laws." *Whren* v. *United States*, 517 U.S. 806, 813 (1996). Those guarantees protect against abusive acquisition of cell-site records—just as with acquisition of banking records or pen-register records of numbers dialed.

Petitioner states (Br. 56-57) that investigators act unreasonably by requesting cell-site data spanning the weeks surrounding a crime. But collection of data before and after an unsolved crime is not arbitrary. Because cell-site records cannot identify an individual's exact location within a tower's coverage area, several weeks of data can help establish whether an individual's phone frequently connects to that tower—which could be "relevant" in determining whether the individual was at the crime scene or instead "had other reasons for being in that neighborhood." J.A. 128. Access to multiple weeks of data can also help officers confirm or refute

the possibility that the suspect frequently loans his phone to others, and did not possess it at the relevant time, thus exonerating the innocent. In any event, as with any demand for third-party records, courts can step in if law enforcement requests are excessive. See p. 45, *infra*.

Ultimately, if the quantity of information now available in third-party business records raises novel privacy concerns, the proper body to address them is the legislature. Members of this Court have recognized that "concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions." *Jones*, 565 U.S. at 427 (Alito, J., concurring in the judgment). The Fourth Amendment cannot prevent private parties from collecting and using data about their customers, but "[a] legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." *Id.* at 429-430. If Congress and state legislatures share petitioner's concern about the type and quantity of information collected by cell-service providers and other third parties, those legislators can pass laws to limit the collection, use, or dissemination of that data. Rather than distort or arbitrarily limit Fourth Amendment doctrine, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative." *Id.* at 429.

Even absent action by the legislature, the public may persuade third-party providers to alter their conduct to protect privacy interests. Providers' decisions to keep records of tower usage spanning months or years stems not from technological necessity, but from business con-

siderations. Companies thus may yield to customer demands for privacy. See, *e.g.*, EPIC Amicus Br. 31-34 (describing how Apple altered the location data it collected after facing a public backlash to its "surreptitious location tracking"); *Fifth Circuit In re Application*, 724 F.3d at 615 ("[C]ell phone users may reasonably want their location information to remain private, * * * [b]ut the recourse for these desires is in the market or the political process: in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections."). A variety of constraints accordingly may shield certain information conveyed to a third party from further disclosure.

B. The Government Did Not Obtain The Cell-Site Records By Trespassing On A Constitutionally Protected Area

Petitioner alternatively contends (Br. 32) that the government's acquisition of his providers' cell-site records impermissibly intruded on his private papers under "[a] property-based [Fourth Amendment] analysis." That argument is not properly presented here because petitioner did not press it below, the court of appeals did not pass upon it, and petitioner did not raise the claim in his petition for a writ of certiorari. See *Jones*, 565 U.S. at 413. In any event, petitioner's argument that the government's acquisition of historical cell-site records constituted a trespassory search lacks merit.

1. Petitioner's property-based argument falters at the first step because he cannot establish a cognizable property interest in his providers' records of which cell towers they used to connect his calls. Petitioner did not create those records and has no right to control their content. Although petitioner now maintains (Br. 32-35)

that the providers' cell-site records are his own "papers" or "effects," he "stipulate[d] and agree[d]" at trial that they instead were "authentic and accurate business records of [MetroPCS and Sprint]." J.A. 51; see *Christian Legal Soc'y* v. *Martinez*, 561 U.S. 661, 677 (2010) (parties are "bound by the factual stipulations [they] submit[]").

In asserting that he has a property interest in his providers' cell-site records, petitioner again relies on 47 U.S.C. 222, which he maintains prohibits disclosure of cell-site information "without 'express prior authorization of the customer.'" Pet. Br. 11 (citation omitted). As explained, pp. 21-22, *supra*, petitioner misreads the statute: Section 222 permits disclosure of cell-site records in a variety of circumstances without a customer's consent. 47 U.S.C. 222(c)(1) and (d)(1)-(4). The statute accordingly cannot bear the weight petitioner places on it in his novel attempt to establish that he has property rights in his providers' business records. See Pamela Samuelson, *Privacy As Intellectual Property*, 52 Stan. L. Rev. 1125, 1130-1131 (2000) ("Although the law often protects the interests of individuals against wrongful uses or disclosures of personal data, the rationale for these legal protections has not historically been grounded on a perception that people have property rights in personal data as such.") (footnote omitted).

2. Even if Section 222 created certain property rights in cell-site information, petitioner cannot establish that the government's acquisition of the records invades any interest protected by the statute. Section 222 authorizes disclosure of cell-site records without the customer's consent in accordance with the SCA. See 47 U.S.C. 222(c)(1) (permitting disclosure "as required by law"). And cell-service providers expressly reserve

their rights to collect cell-site information and disclose that data in response to court orders. See p. 3 n.1, *supra* (citing privacy policies). The government's acquisition of the providers' business records is therefore consistent with any conceivable property rights petitioner might have in those records.

II. IF THE GOVERNMENT'S ACQUISITION OF CELL-SITE RECORDS WAS A SEARCH OF PETITIONER, IT WAS REASONABLE UNDER THE FOURTH AMENDMENT

Even if petitioner could establish that the government's acquisition of MetroPCS's and Sprint's business records pursuant to an SCA order qualified as a Fourth Amendment search of him, the government's action was constitutionally reasonable.[11] As this Court recently observed, "[t]he Fourth Amendment's proper function is to constrain, not against all intrusions as such, but against intrusions which are not justified in the circumstances, or which are made in an improper manner." *Maryland* v. *King*, 133 S. Ct. 1958, 1969 (2013) (brackets in original; citation omitted). Thus, "[a]s the text of

---

[11] Petitioner suggests (Br. 48) that the Court avoid decision on this issue and instead remand for the court of appeals to consider whether any search of him was reasonable. But the question presented asks whether the Fourth Amendment permits the government to acquire cell-site records without a warrant, Pet. i, and that question cannot be answered without resolving whether any search was constitutionally reasonable. The government raised the reasonableness argument below and in its brief in opposition, see Gov't C.A. Br. 37-40; Br. in Opp. 22-26, and that issue accordingly is properly presented here. See *Granfinanciera, S. A.* v. *Nordberg*, 492 U.S. 33, 38–39 (1989). The Eleventh Circuit has agreed with the government's position that the warrantless acquisition of historical cell-site records is reasonable. See *Davis*, 785 F.3d at 516-518. The Court should resolve that question to provide "clear guidance to law enforcement." *Riley*, 134 S. Ct. at 2491.

the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'" *Ibid.* (citation omitted).

Applying that standard here, the Fourth Amendment permits the government's acquisition of cell-site records pursuant to a judicial order authorized by the SCA. That action falls within the well-recognized permissibility of using compulsory process to obtain information. And a traditional balance of interests further demonstrates that the government's conduct was reasonable.

A. Law Enforcement Agents Need Not Obtain A Warrant To Conduct Searches Using Compulsory Process

1. This Court has long recognized that the Fourth Amendment applies to the use of subpoenas and other forms of government action that result in "the orderly taking under compulsion of process." *United States* v. *Morton Salt Co.*, 338 U.S. 632, 652 (1950); see, *e.g.*, *United States* v. *Dionisio*, 410 U.S. 1, 11-12 (1973) (grand jury subpoena); *McPhaul* v. *United States*, 364 U.S. 372, 382-383 (1960) (legislative subpoena); *Oklahoma Press Publ'g Co.* v. *Walling*, 327 U.S. 186, 208-209 (1946) (*Oklahoma Press*) (administrative subpoena). In applying the Fourth Amendment reasonableness standard in this context, the Court has concluded that subpoenas for records do not require a warrant based on probable cause, even when challenged by the party to whom the records belong. See *Miller*, 425 U.S. at 446; see also *Oklahoma Press*, 327 U.S. at 208-209. Instead, the Fourth Amendment permits the government to acquire documents by subpoena so long as "the investigation is authorized by Congress, is for a purpose Congress can order, * * * the documents sought are rele-

vant to the inquiry," and the "specification of the documents to be produced [is] adequate, but not excessive, for the purposes of the relevant inquiry." *Oklahoma Press*, 327 U.S. at 209; see *Donovan* v. *Lone Steer, Inc.*, 464 U.S. 408, 415 (1984) ("[T]he Fourth Amendment requires that the subpoena be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.") (citation omitted).

The Court has identified several reasons why the Fourth Amendment does not require a warrant for the government to obtain evidence using compulsory process. That conduct represents a lesser degree of intrusion than the kinds of searches that typically require a warrant because the subpoena recipient rather than the government finds and produces the record. See *Donovan*, 464 U.S. at 414 (observing that governmental action in "mak[ing] nonconsensual entries into areas not open to the public" is "quite different from * * * governmental action" in seeking the production of records); see also *Dionisio*, 410 U.S. at 10. In addition, the subpoena recipient has an "opportunity to present objections" before producing the records, which further minimizes the intrusion. *Oklahoma Press*, 327 U.S. at 195; see *Donovan*, 464 U.S. at 416; see also *City of Los Angeles* v. *Patel*, 135 S. Ct. 2443, 2453-2454 (2015) (explaining the benefits of pre-compliance review).

On the other side of the balance, the Court has recognized that the government has a significant interest in acquiring records through compulsory process at the early stage of an investigation, before probable cause exists to support issuance of a warrant. See *Oklahoma Press*, 327 U.S. at 213 (observing that a warrant requirement in this context "would stop much if not all of

investigation in the public interest at the threshold of inquiry," rendering it "substantially impossible" to "effective[ly] discharge * * * the duties of investigation"). The government's ability to investigate and prosecute crime would be severely hindered if it were "required to justify the issuance of a * * * subpoena by presenting evidence sufficient to establish probable cause" when "the very purpose of requesting the information is to ascertain whether probable cause exists." *United States* v. *R. Enterprises, Inc.*, 498 U.S. 292, 297 (1991). This Court has accordingly recognized that the use of a subpoena to obtain a third party's records pertaining to an individual is "a proper and long-standing law enforcement technique" that "does not violate the Fourth Amendment rights of [the individual] under investigation." *Miller*, 425 U.S. at 444.

2. The government's acquisition of cell-site records pursuant to a court order authorized by the SCA falls within the authority this Court has recognized for "subpoena[s] or order[s] authorized by law and safeguarded by judicial sanction." *Oklahoma Press*, 327 U.S. at 208. Section 2703(d) orders share the same features as other forms of compulsory process that have prompted the Court to find Fourth Amendment requirements satisfied without a warrant: the recipient, not the government, locates and produces the records; the recipient may challenge the order in court before complying, see 18 U.S.C. 2703(d); and the government often relies on Section 2703(d) orders at the preliminary stage of an investigation before it has developed probable cause.

Indeed, the SCA provides substantially greater privacy protections than an ordinary subpoena. See *Davis*, 785 F.3d at 505-506 (describing SCA privacy-protection provisions). In particular, Section 2703(d) "raises the

bar" as compared to other forms of compulsory process by requiring the government to establish "specific and articulable facts showing that there are reasonable grounds to believe that * * * the records or other information sought[] are relevant and material to an ongoing criminal investigation," 18 U.S.C. 2703(d). *Davis*, 785 F.3d at 505-506. The SCA provides further protection by requiring court approval, which ensures that a neutral judicial officer agrees that the request is appropriate in scope and justification. Because "[t]he SCA goes above and beyond the constitutional requirements regarding compulsory subpoena process," *id.* at 506, the government's acquisition of business records pursuant to a valid Section 2703(d) order does not violate the Fourth Amendment.

3. Petitioner contends (Br. 51-53) that the Fourth Amendment permits the warrantless acquisition of a third party's records pursuant to subpoena only when an individual to whom the records pertain holds no "reasonable expectation of privacy" in the records. This Court's cases do not support petitioner's proposed limitation, and acceptance of his argument would impose serious burdens on investigations.

Petitioner identifies no case in which this Court has held that certain classes of business records are exempt from the subpoena standard because they contain sensitive information about the business's customers.[12]

---

[12] Although petitioner acknowledges (Br. 52) that the Court has permitted the government to subpoena third parties for records pertaining to their customers, he contends that the customers had no legitimate privacy expectation. But that is because the Court applied the third-party doctrine, which equally establishes here that petitioner has no Fourth Amendment privacy expectation is his cell-service providers' records. See pp. 15-41, *supra*.

The subpoena standard itself may impose more stringent requirements depending on the nature of the requested documents. See *Oklahoma Press*, 327 U.S. at 209 ("[R]elevancy and adequacy or excess in the breadth of the subpoena are matters variable in relation to the nature, purposes and scope of the inquiry."). For example, "[s]pecial problems of privacy * * * might be presented by subpoena of a personal diary," which would necessitate a careful review to ensure the subpoena is "narrowly drawn and seek[s] only documents of unquestionable relevance." *Fisher* v. *United States*, 425 U.S. 391, 401 n.7 (1976); see *United States* v. *Bennett*, 409 F.2d 888, 897 (2d Cir. 1969) (Friendly, J.) (distinguishing between a personal diary that may contain large quantities of irrelevant information and a diary "whose cover page bore the title 'Robberies I Have Performed'"), cited by *Fisher*, 425 U.S. at 401 n.7. But courts have rejected petitioner's contention that a warrant is required to subpoena sensitive records held by third parties, instead holding that the subpoena standard's reasonableness requirement sufficiently safeguards any privacy expectations that exist. See, *e.g.*, *United States* v. *Zadeh*, 820 F.3d 746, 758 (5th Cir. 2016) (upholding subpoena for a physician's medical records that "implicat[ed] privacy interests of patients," but "narrowly confining the scope of production to the ongoing government investigation and placing all produced medical records under seal"); *In re Subpoena Duces Tecum*, 228 F.3d 341, 349 (4th Cir. 2000) (rejecting challenge to subpoena for medical records, but observing that "[t]he value of constraining governmental power, which [the physician] has urged through his misplaced probable cause argument, is nevertheless recognized in the judicial supervision of subpoenas").

Petitioner suggests (Br. 52) that Section 2703(d) orders are unreasonable because the government need not provide notice to the individual to whom the records pertain. As a general matter, this Court has rejected the argument that the Fourth Amendment requires "notice of subpoenas issued to third parties * * * to allow a target to prevent an unconstitutional search or seizure." *SEC*, 467 U.S. at 743. Even if a target has a limited expectation of privacy in records held by a third party, courts can accommodate that interest when assessing the justification and scope of a request for information, as Section 2703(d) requires. Judicial authorization in advance of the intrusion provides appropriate protection when notice to the target would frustrate the investigative purpose. See, *e.g.*, *Dalia* v. *United States*, 441 U.S. 238, 247-248 (1979). And altering the Fourth Amendment standard to require a warrant would not address petitioner's notice concern. The warrant would be served on the provider, not the target, and in any event, notice of a warrant is neither an inflexible Fourth Amendment requirement, see *Katz*, 389 U.S. at 355 n.16, nor a basis for a pre-enforcement challenge, see *United States* v. *Grubbs*, 547 U.S. 90, 98-99 (2006).

Petitioner's proposed revision of the constitutional standard for subpoenas would impede longstanding investigative practices. This Court has recognized that the government's use of compulsory process is "necessary to the administration of justice." *Dionisio*, 410 U.S. at 10 (citation omitted). Petitioner himself shrinks from the extreme implications of his argument, suggesting (Br. 53 n.40) that "the Court need not address whether different rules are appropriate for subpoenas issued by a grand jury." But the Court has held that administrative subpoenas are analogous to their grand-

jury counterparts, *Morton Salt*, 338 U.S. at 642-643, and has applied the same constitutional standard to all forms of compulsory process, *Dionisio*, 410 U.S. at 10-11. The reasonableness standard that applies to subpoenas demonstrates that the government did not violate the Fourth Amendment in obtaining business records pursuant to a valid order under Section 2703(d).

B. A Traditional Balancing Of Interests Further Supports The Constitutionality Of A Section 2703(d) Order

Traditional standards of Fourth Amendment reasonableness independently confirm that a Section 2703(d) court order is a reasonable mechanism for obtaining historical cell-site records. In deciding whether a warrantless search is permissible, this Court "balance[s] the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable." *King*, 133 S. Ct. at 1970 (citation omitted). Congress struck a constitutionally permissible balance in enacting the SCA.

1. As discussed above, under traditional Fourth Amendment standards, petitioner had no legitimate expectation of privacy in the third-party business records at issue here. But even if this Court were to depart from that settled framework, petitioner could at most assert only a diminished expectation of privacy in those records. Cf. Pet. Br. 38 (treating disclosure of information to a third party as "one factor" that affects privacy expectations). Petitioner did not create the records, he does not possess them, and he has no control over their contents.

To the extent the providers' collection of information about petitioner's proximity to their cell towers infringed his privacy expectations, that conduct occurred

without governmental involvement. And the government's subsequent acquisition of the providers' records in accordance with Section 2703(d) constituted an "orderly taking under compulsion of process." *Morton Salt*, 338 U.S. at 652. The statutory protections in the SCA further minimized any privacy invasion by prohibiting "[a]ny willful disclosure" of cell-site information not "made in the proper performance of" governmental functions. 18 U.S.C. 2707(g); see *King*, 133 S. Ct. at 1980 (noting that "a statutory or regulatory duty to avoid unwarranted disclosures generally allays . . . privacy concerns") (citation and internal quotation marks omitted). The use of a Section 2703(d) order to obtain cell-service providers' business records thus involves a "minimal intrusion[]" and "diminished expectations of privacy"—both of which "may render a warrantless search or seizure reasonable." *King*, 133 S. Ct. at 1969 (citation omitted).

2 On the other side of the reasonableness balance, the government has a compelling interest in obtaining cell-site records using a Section 2703(d) court order, rather than a warrant, because, like other investigative techniques that involve seeking information about a crime from third parties, this evidence is "particularly valuable during the early stages of an investigation, when the police [may] lack probable cause and are confronted with multiple suspects." *Davis*, 785 F.3d at 518. "[Section] 2703(d) orders—like other forms of compulsory process not subject to the search warrant procedure—help to build probable cause against the guilty, deflect suspicion from the innocent, aid in the search for truth, and judiciously allocate scarce investigative resources." *Ibid.*

Examples illustrate the important role cell-site information plays in helping law enforcement agents develop leads and solve crimes. In one case, the FBI determined that someone was using a home computer to distribute and download child pornography, but each of the four adults who regularly used that computer denied responsibility for the crime. See *United States* v. *Reynolds*, 626 Fed. Appx. 610, 612 (6th Cir. 2015), petition for cert. pending, No. 16-8574 (filed Dec. 10, 2015). The FBI obtained cell-site records that revealed that three of the four adults used cell towers that were "geographically inconsistent" with their being near the computer at times when child pornography was downloaded, while the fourth adult "used cell towers that were consistent with his being at the residence during the download periods." *Ibid.* The records accordingly helped the government eliminate three suspects and identify the perpetrator.

In another example, cell-site records helped investigators identify the person who shot into the home of a federal judge. "The police had no eyewitnesses and a very large pool of suspects, including many litigants and defendants who had appeared before the judge," but with the aid of court-issued orders for cell-site information pertaining to some "possible suspects," the police acquired "a general idea of the location of the phones," which "allowed agents to exclude certain innocent people and pursue leads that eventually led to the arrest of the alleged shooter." *Geolocation Technology and Privacy: Hearing Before the H. Comm. on Oversight and Government Reform*, 114th Cong., 2d Sess. 4-5 (2016) (statement of Richard Downing, Acting DAAG, Computer Crime and Intellectual Property Section, U.S. Department of Justice).

States and the federal government unquestionably have an "interest in apprehending violators," *United States* v. *Knights*, 534 U.S. 112, 121 (2001), and in doing so as quickly as possible. See *United States* v. *Salerno*, 481 U.S. 739, 750-751 (1987). Bringing the guilty to justice vindicates the law, protects the public, and provides closure to victims. These benefits lie at the very heart of the government's responsibility to maintain order and shield its citizens from harm—and they support the reasonableness of the SCA orders at issue here.

3. That conclusion gains additional force from the legislative judgment embodied by the SCA. This Court has "be[en] reluctant to decide that a search * * * authorized by Congress was unreasonable," *United States* v. *Di Re*, 332 U.S. 581, 585 (1948), particularly when "nothing in the Court's prior cases indicat[es] that under the Fourth Amendment a warrant is required," *United States* v. *Watson*, 423 U.S. 411, 416-417 (1976). In enacting the SCA, Congress specifically considered Fourth Amendment principles and this Court's precedents. See H.R. Rep. No. 647, 99th Cong., 2d Sess. 72 (1986) (1986 House Report) (observing that "records maintained by third parties" generally "have no special privacy or confidentiality protection"). Congress selected the Section 2703(d) standard after determining that "an intermediate standard" that is "higher than a subpoena, but not a probable cause warrant" would "guard against 'fishing expeditions' by law enforcement" while ensuring access to cell-service providers' records pertaining to their customers in appropriate circumstances. H.R. Rep. No. 827, 103d Cong., 2d Sess. Pt. 1, at 31 (1994). The SCA thus "represents a judgment by Congress that it is not unreasonable under the Fourth Amendment" for the government to obtain cell-

site records in accordance with the statutory procedures Congress enacted—a consideration entitled to significant weight. *Watson*, 423 U.S. at 415; see *Jones*, 565 U.S. at 429-430 (Alito, J., concurring in the judgment).

Petitioner contends (Br. 50) that Congress may not have "anticipate[d] the contemporary ubiquity of cell phones" when it chose the Section 2703(d) standard. But Congress designed the statute to respond to "dramatic changes in new computer and telecommunications technologies," which it recognized included cell phones. S. Rep. No. 541, 99th Cong., 2d Sess. 1-2 (1986) (Senate Report); see 1986 House Report 18. Congress understood that cell-phone technology works by "send[ing] signals over the air on a radio frequency to a cell site." 1986 House Report 20; Senate Report 9. And Congress specifically applied the Section 2703(d) standard to all non-content records cell-service providers might keep pertaining to their customers, concluding that the standard "represents a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies." Senate Report 5.

Congress has had numerous opportunities to reconsider the balance it struck in Section 2703(d)—including as applied specifically to cell-site information.[13] In 2000, for example, Congress considered—but ultimately did not enact—a bill that would have amended Section 2703

---

[13] Congress did alter the Section 2703(d) standard in 1994 to make it harder for the government to obtain non-content records by requiring the government to offer "specific and articulable facts" and seek only records that may be "material" to an ongoing investigation. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, Tit. II, § 207(a), 108 Stat. 4292.

to require a showing of probable cause for "mobile electronic information generated by and disclosing the current physical location of a subscriber's equipment." Digital Privacy Act of 2000, H.R. 4987, 106th Cong., 2d Sess. § 6, at 4 (2000). And earlier this year, the House referred a bill to committee that would allow the government to obtain cell-site records using search warrants but not Section 2703(d) orders. See Geolocation Privacy and Surveillance Act, H.R. 1062, 115th Cong., 1st Sess. §§ 2, 5 (2017). Congress considered similar proposals in prior iterations of that bill. See, *e.g.*, Geolocational Privacy and Surveillance Act, S. 237, 114th Cong., 1st Sess. §§ 2, 5 (2015); Geolocational Privacy and Surveillance Act, H.R. 1312, 113th Cong., 1st Sess. §§ 2, 5 (2013). Congress's continued attention to the appropriate balance between privacy interests and the needs of law enforcement in the face of rapidly evolving technology reinforces the reasonableness of the Section 2703(d) standard.

III. PETITIONER CORRECTLY CONCEDES THAT THE GOVERNMENT DOES NOT VIOLATE THE FOURTH AMENDMENT BY ACQUIRING SHORTER-TERM CELL-SITE RECORDS

For the reasons set forth above, the court of appeals correctly held that the government's warrantless acquisition of all the cell-site records pertaining to petitioner's phone complied with the Fourth Amendment.[14] But if the Court were to conclude that requests for long-

---

[14] If the Court disagrees and concludes that the government violated petitioner's Fourth Amendment rights it should remand to allow the court of appeals to consider the government's arguments that the good-faith exception to the exclusionary rule applies and that any error in admitting the cell-site data was harmless. See Gov't C.A. Br. 40-47.

term cell-site data require a warrant, it should confirm that the Section 2703(d) order directed at Sprint—which sought seven days of records and resulted in the production of two days of data—was constitutional.

Petitioner acknowledges that "there is some period of time for which the government may obtain a person's historical [cell-site information] free from Fourth Amendment scrutiny, because the duration is too brief to implicate the person's reasonable privacy interest." Br. 30 (brackets, citation, and internal quotation marks omitted). That concession follows from petitioner's recognition (Br. 30-31) that investigators using traditional surveillance techniques frequently obtain information about an individual's location and movements during discrete time periods. "[R]elatively short-term monitoring of a person's movements" therefore "accords with expectations of privacy that our society has recognized as reasonable." *Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment).

Applying that analysis, agents did not need a warrant to request seven days of cell-site information from Sprint. Law enforcement agents regularly surveil suspects for a week or more. See, *e.g.*, *Young* v. *Owens*, 577 Fed. Appx. 410, 412 (6th Cir. 2014) ("[s]everal weeks of surveillance" of a store); *United States* v. *Gaskins*, 690 F.3d 569, 574, 577 (D.C. Cir. 2012) ("weeks of surveillance" of "numerous locations * * * using stationary vans, moving cars, and a mounted pole camera"); *United States* v. *Johnson*, 480 Fed. Appx. 835, 837 (6th Cir. 2012) (suspect's residence was under visual surveillance "for five to six weeks and he was seen there on a daily basis"); *United States* v. *Gramlich*, 551 F.2d 1359, 1360-1361 & n.7, 1362 (5th Cir.) ("continual surveillance of [defendant's] activities" for "over three weeks"), cert.

denied, 434 U.S. 866 (1977); *Shades Ridge Holding Co.* v. *Commissioner of Internal Revenue*, 23 T.C.M. (CCH) 1665 (1964) ("close surveillance of [suspect] and of his activities" that "often was continuous, all day, for 6 days a week" over several months).

Using traditional techniques, officers can acquire extensive information about an individual's movements. In one case, for example, officers conducted "more than one week of detailed surveillance" and determined that the suspect's movements "followed a set pattern" that included his departure from his home in a particular make of car; his arrival at a nearby building where "he would place window tinting film on his car windows"; his entrance on "Interstate 64 westbound toward Mechanicsville"; his exit from the interstate, where he affixed "a new license plate"; his return on the same interstate; his "driv[ing] back and forth on Route 360, stopping in parking lots adjacent to two different banks but never exiting his car"; and then finally his returning home. *United States* v. *Caraballo*, 384 Fed. Appx. 285, 287-288, 290 (4th Cir. 2010) (per curiam). The seven days of cell-site information from Sprint here—which contained far less precise location information—surely threatened no greater intrusion on petitioner's asserted privacy interests (and probably far less) than what officers could have obtained "using previously available techniques." *Jones*, 565 U.S. at 431 (Alito, J., concurring in the judgment). In no circumstance, therefore, did the Section 2703(d) order directed at Sprint violate the Fourth Amendment.

CONCLUSION

The judgment of the court of appeals should be affirmed.

Respectfully submitted.

NOEL J. FRANCISCO
Solicitor General
KENNETH A. BLANCO
Acting Assistant Attorney General
MICHAEL R. DREEBEN
Deputy Solicitor General
ELIZABETH B. PRELOGAR
Assistant to the Solicitor General
JENNY C. ELLICKSON
Attorney

SEPTEMBER 2017

APPENDIX A

1. U.S. Const. Amend. IV provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

2. 18 U.S.C. 2703 provides:

Required disclosure of customer communications or records

(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a sub-

scriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there

are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.—No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) REQUIREMENT TO PRESERVE EVIDENCE.—

(1) IN GENERAL.—A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) PERIOD OF RETENTION.—Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional

90-day period upon a renewed request by the governmental entity.

(g) PRESENCE OF OFFICER NOT REQUIRED.—Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

3. 47 U.S.C. 222 provides:

Privacy of customer information

(a) In general

Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.

(b) Confidentiality of carrier information

A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

(c) Confidentiality of customer proprietary network information

(1) Privacy requirements for telecommunications carriers

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

(2) Disclosure on request by customers

A telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.

(3) Aggregate customer information

A telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service may use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1). A local exchange carrier may use, disclose, or permit access to aggregate customer information other than for purposes described in paragraph (1) only if it provides such aggregate information to other carriers or persons on

reasonable and nondiscriminatory terms and conditions upon reasonable request therefor.

(d) Exceptions

Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents—

(1) to initiate, render, bill, and collect for telecommunications services;

(2) to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services;

(3) to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service; and

(4) to provide call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d) of this title) or the user of an IP-enabled voice service (as such term is defined in section 615b of this title)—

(A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;

(B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or

(C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.

(e) Subscriber list information

Notwithstanding subsections (b), (c), and (d) of this section, a telecommunications carrier that provides telephone exchange service shall provide subscriber list information gathered in its capacity as a provider of such service on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any format.

(f) Authority to use location information

For purposes of subsection (c)(1) of this section, without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to—

(1) call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d) of this title) or the user of an IP-enabled voice service (as such term is defined in section 615b of this title), other than in accordance with subsection (d)(4) of this section; or

(2) automatic crash notification information to any person other than for use in the operation of an automatic crash notification system.

(g) Subscriber listed and unlisted information for emergency services

Notwithstanding subsections (b), (c), and (d) of this section, a telecommunications carrier that provides telephone exchange service or a provider of IP-enabled voice service (as such term is defined in section 615b of this title) shall provide information described in subsection (i)(3)(A)[1] of this section (including information pertaining to subscribers whose information is unlisted or unpublished) that is in its possession or control (including information pertaining to subscribers of other carriers) on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions to providers of emergency services, and providers of emergency support services, solely for purposes of delivering or assisting in the delivery of emergency services.

(h) Definitions

As used in this section:

(1) Customer proprietary network information

The term "customer proprietary network information" means—

(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecom-

---

[1] So in original. Probably should be subsection "(h)(3)(A)".

munications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;

except that such term does not include subscriber list information.

(2) Aggregate information

The term "aggregate customer information" means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

(3) Subscriber list information

The term "subscriber list information" means any information—

(A) identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and

(B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.

(4) Public safety answering point

The term "public safety answering point" means a facility that has been designated to receive emer-

gency calls and route them to emergency service personnel.

(5) Emergency services

The term "emergency services" means 9-1-1 emergency services and emergency notification services.

(6) Emergency notification services

The term "emergency notification services" means services that notify the public of an emergency.

(7) Emergency support services

The term "emergency support services" means information or data base management services used in support of emergency services.

APPENDIX B

The illustrative map in Figure 2 at p. 26, *supra*, is intended to show the approximate density and variety of establishments in the area where cell-site records placed petitioner's phone around the time of a robbery of a Radio Shack at 13330 E. Jefferson Ave., Detroit, Michigan, 48215, on December 13, 2010. See Pet. App. 80a-82a, 86a; see also J.A. 57-60 (testimony explaining the creation of the map appearing in Government Exhibit 57, reproduced at Pet. App. 86a). The illustrative map was created using Google Maps' My Maps tool. See https://www.google.com/maps/about/mymaps/. It reflects Google's map, satellite, and directory information as of September 25, 2017.

The illustration covers the region between two cell towers that petitioner's phone connected to the morning of the robbery, based on the cell tower and sector locations from the government's trial exhibit reproduced at Pet. App. 86a; see also p. 25, *supra* (reproducing a portion of that exhibit). The locations of the cell towers and the lines depicting the cell sectors in the illustrative map are based on their locations on the exhibit at Pet. App. 86a. The cell towers' coverage area shown on the illustrative map is approximate.

The icons on the map represent establishments in that area, based on Google Maps' satellite imagery and directory labels. Buildings not labeled by Google were identified from Google's satellite and street imagery; most were single-family homes or apartment buildings. Buildings or structures that appeared to be empty or abandoned were not counted, such that the illustrative map errs on the side of under-inclusion.

RECORD
AND
BRIEFS

No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

—v.—

UNITED STATES OF AMERICA,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

REPLY BRIEF FOR PETITIONER

Nathan Freed Wessler
Ben Wizner
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004

David D. Cole
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
915 15th Street, NW
Washington, DC 20005

Cecillia D. Wang
Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111

Harold Gurewitz
Counsel of Record
GUREWITZ & RABEN, PLC
333 W. Fort Street, Suite 1400
Detroit, MI 48226
(313) 628-4733
hgurewitz@grplc.com

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
AMERICAN CIVIL LIBERTIES UNION FUND OF MICHIGAN
2966 Woodward Ave.
Detroit, MI 48201

Jeffrey L. Fisher
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

REPLY BRIEF FOR PETITIONER 1

I. LAW ENFORCEMENT'S ACQUISITION OF LONGER-TERM HISTORICAL CSLI IS A SEARCH 2

A. People Have A Reasonable Expectation Of Privacy In Longer-Term Historical CSLI. 2

B. Procuring CSLI Intrudes on People's "Papers" Under the Fourth Amendment 14

C. The Government's Theory Would Negate Fourth Amendment Protection For A Wide Range Of Vital Privacy Interests In The Digital Age 16

II. WARRANTLESS SEARCH OF LONGER-TERM HISTORICAL CSLI IS UNREASONABLE UNDER THE FOURTH AMENDMENT 18

A. The Subpoena Power Does Not Allow The Government To Obtain Records Held By A Third Party In Which There Is A Reasonable Expectation Of Privacy 18

B. Principles Of Fourth Amendment Reasonableness Require A Warrant... 22

C. Congressional Inaction Is Irrelevant Here 24

CONCLUSION 25

TABLE OF AUTHORITIES

CASES

Alderman v. United States, 394 U.S. 165 (1969) 22

Couch v. United States, 409 U.S. 332 (1973) 19, 21

Dickman v. C.I.R., 465 U.S. 330 (1984) 15

Donovan v. Lone Steer, Inc., 464 U.S. 408 (1984) 19

Ex Parte Jackson, 96 U.S. 727 (1877) 16

Fisher v. United States, 425 U.S. 391 (1976) 19, 20

Ford v. State,
477 S.W.3d 321 (Tex. Crim. App. 2015) 24

Hoffa v. United States, 385 U.S. 293 (1972) 11

Kyllo v. United States, 533 U.S. 27 (2001) 2, 3, 5

Lebron v. Nat'l R.R. Passenger Corp.,
513 U.S. 374 (1995) 14

Maryland v. King, 133 S. Ct. 1958 (2013) 22

Minnesota v. Olson, 495 U.S. 91 (1990) 11

Pension Ben. Guar. Corp. v. LTV Corp.,
496 U.S. 633 (1990) 24

Riley v. California, 134 S. Ct. 2473 (2014) .....*passim*

See v. City of Seattle, 387 U.S. 541 (1967) 21

Shades Ridge Holding Co. v. CIR,
23 T.C.M. (CCH) 1665 (1964) 13

Smith v. Maryland, 442 U.S. 735 (1979) 2, 7, 8, 9

State v. Ford, 454 S.W.3d 407 (Mo. Ct. App. 2015) ... 6

State v. Roberts,
No. 13-009778CF10A (Fla. 17th Cir. Ct. May 3, 2016) 6

United States v. Brown,
2017 WL 4216979 (D. Neb. 2017) 23

United States v. Gaskins,
690 F.3d 569 (D.C. Cir. 2012) 13

United States v. Gramlich,
551 F.2d 1359 (5th Cir. 1977) 13

United States v. Jacobsen, 466 U.S. 109 (1984). 11, 12

United States v. Johnson,
480 F. App'x 835 (6th Cir. 2012) 13

United States v. Jones, 565 U.S. 400 (2012) .....*passim*

United States v. Karo, 468 U.S. 705 (1984) 5

United States v. Miller, 425 U.S. 435 (1976) ....*passim*

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 20

United States v. Williams,
504 U.S. 36 (1992) 14

Young v. Owens, 577 F. App'x 410 (6th Cir. 2014) .. 13

U.S. CONSTITUTION & STATUTES

U.S. Const. amend. IV .....*passim*

18 U.S.C. § 2702(a)(3) 12

18 U.S.C. § 2702(c)(4) 12

18 U.S.C. § 2703(d) 22, 23, 24

47 U.S.C. § 222 ..... 9, 10

47 U.S.C. § 222(c)(1) 10

47 U.S.C. § 222(c)(3) 10
47 U.S.C. § 222(d)(4) 10
47 U.S.C. § 222(f) 10

RULES

Fed. R. Evid. 803(6) 15

LEGISLATIVE MATERIALS

Email Privacy Act, H.R. 699, 114th Cong. (2015) ... 24

OTHER AUTHORITIES

Google Terms of Service,
https://www.google.com/policies/terms 17

Joseph Hoy, *Forensic Radio Survey Techniques for Cell Site Analysis* (2015) 7

REPLY BRIEF FOR PETITIONER

Cell phones (and related mobile devices) are increasingly indispensable tools of modern life. It is essential that people not only own such devices but also that they carry them virtually all the time, wherever they go. As the Technology Companies explain, it is an inescapable fact that such devices reveal locational information to service providers "by dint of their mere operation." Tech. Cos. Br. 11.

The government argues that the consequence of this technological landscape is that Americans no longer have any right to privacy in the aggregation of their movements over time. Simply by using cell phones, the government maintains, the populace gives law enforcement constitutionally unchecked authority to collect a detailed record of every person's historical whereabouts—without probable cause, a warrant, or any Fourth Amendment protection whatsoever.

This cannot be right. The American people have a reasonable expectation that the details of their minute-by-minute travel over time remain private, as they always have been. A proper understanding of the Fourth Amendment renders law enforcement's procurement of longer-term CSLI a "search." And the only way such a search can be reasonable is with a warrant.

I. LAW ENFORCEMENT'S ACQUISITION OF LONGER-TERM HISTORICAL CSLI IS A SEARCH.

A. People Have A Reasonable Expectation Of Privacy In Longer-Term Historical CSLI.

Citing principally to *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), the government urges the Court to ignore the sea change in technology that made possible the search of 127 days of petitioner's location data, and to decide this case through wooden application of legal principles from a bygone era. *See* Resp. Br. 32-33. But this Court's more recent precedent dictates that the government cannot capitalize on new technology to shrink privacy. And even on their own terms, *Smith* and *Miller* do not control here.

1. In the face of technological change, the Fourth Amendment "assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States*, 533 U.S. 27, 34 (2001); *see also Riley v. California*, 134 S. Ct. 2473, 2495 (2014) (warrant requirement applies to cell phones seized incident to arrest to safeguard "the privacies of life" previously protected by that requirement). Five concurring Justices applied that principle in *United States v. Jones* to hold that GPS tracking constitutes a search because people never expected before the advent of modern location-tracking technology that compilations of their movements for weeks on end would be readily accessible to government agents. 565 U.S. 400, 429-31 (2012) (Alito, J., concurring in the judgment).

As with the GPS technology in *Jones*, the advent of cellular service technology has given the government access to locational information previously unimaginable, and has so lowered the cost of obtaining this information as to remove all practical impediments to massive incursions on privacy. *See* Tech. Experts Br. 22-25; Elec. Frontier Found. Br. 16 n.32. People have always had a reasonable expectation that no one other than themselves would know everywhere they have traveled for extended periods of time. No one could have decided after the fact to track another person's movements retrospectively, and to instantaneously pluck that historical record out of thin air.

That is what the government says it—and, by extension, state and local police agencies—can now do. Yet neither of its arguments for distinguishing the anti-shrinkage principle in *Jones*, *Kyllo*, and *Riley* holds up.

a. Contrary to the government's contention (Resp. Br. 33), it does not matter that *Jones* and *Kyllo* involved police officers' use of their own technology, whereas here the government is capitalizing on technology deployed by others. The means the government uses to obtain information is sometimes relevant, but so too is the nature of the information obtained. That is why the concurring Justices in *Jones* suggested that the same concerns animating their conclusion that a search took place would have been raised by "surreptitiously activating a stolen vehicle detection system" in Jones's car or conducting GPS tracking of his phone. 565 U.S. at 426, 428. Likewise, the Court in *Riley* applied the full protections of the Fourth Amendment to searches of

cell phones even though the privacy intrusion was purely a function of the storage capacity of the phones themselves; the government used nothing more than its agents' hands and eyes to conduct the searches at issue. 134 S. Ct. at 2480-81.

In a democratic society, it is vital to safeguard a sphere of individual privacy in which people can conduct their affairs free of unwarranted government intrusion. *See Riley*, 134 S. Ct. at 2494-95; *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring). Here, as in *Jones* and *Riley*, the power the government seeks would dramatically unsettle the balance between personal liberty and state power that the Fourth Amendment was intended to preserve. It does not matter whether the government seeks to use its own technology or to leverage a private industry's new technology to conduct surveillance. Either way, the chilling effect would be the same.

b. Nor can the government distinguish *Jones* on the ground that CSLI is substantially less revealing than GPS information. The government's argument based on two individual location points from petitioner's records dating back to 2010 (Resp. Br. 24-27) dramatically understates the privacy stakes at issue.

i. Even when individual points of location data place a person within a relatively large cell site sector, the aggregation of just a small number of such points can reveal significantly more precise information than one point alone. Petr. Br. 24-26. In this case, a limited analysis of petitioner's CSLI data by the American Civil Liberties Union as amicus in the court below determined when petitioner spent the night in an area consistent with his home, and

when he slept in a neighborhood four miles away, as well as his habit of traveling to the same spot in Detroit on Sunday afternoons—an area consistent with the location of his church. 6th Cir. Doc. No. 29, at 11-12. This is the same kind of information that motivated the concurring Justices in *Jones*.

ii. The government's observation that "reasonable inferences or additional evidence" may sometimes be necessary to interpret the significance of CSLI (Resp. Br. 24) makes no difference. This Court has rejected "the novel proposition that inference insulates a search." *Kyllo*, 533 U.S. at 36. The proposition is "blatantly contrary" to the Court's holding in *United States v. Karo*, 468 U.S. 705 (1984), "where the police 'inferred' from the activation of a beeper that a certain can of ether was in the home." *Kyllo*, 533 U.S. at 36.

The possibility that inference or additional evidence may be necessary to interpret location data is also true of the GPS tracking that this Court confronted in *Jones*. Tracking a car to a parking lot will not reveal whether the suspect went to the nearby jewelry store for a robbery, doctor's office for a checkup, or cafe for a meeting with a friend. Corroborating evidence is commonly required. But prolonged GPS tracking nonetheless constitutes a search. *Jones*, 565 U.S. at 429-30 (Alito, J., concurring in the judgment).

iii. The progression of CSLI technology—merging ever closer to the precision of GPS, and bound in the near future to be virtually the same—clinches the applicability of *Jones* to the situation here. Petr. Br. 26-29. The government urges this Court to ignore this progression on the grounds that

(1) "no case" has yet dealt with current technology and (2) CSLI technology "could develop in a different direction." Resp. Br. 27. Neither argument is persuasive.

Courts are *already* adjudicating cases where the government obtained precise historical cell phone location data that relies on carriers' developing ability to "measure[] the radio frequency distance between the telephone and nearby towers, and g[i]ve an estimate of the location of the telephone itself during the call." *State v. Ford*, 454 S.W.3d 407, 410-11 (Mo. Ct. App. 2015); *see also* Br. for Appellee 30 n.10, *United States v. Fulton*, 837 F.3d 281 (3d Cir. 2016) (No. 15-1513), 2015 WL 7423166 (data showed that suspect's phone was "at the very least 1000 feet away" from the scene). Courts are likewise confronting cases involving cell phones' connections to "small cells." In one recent case, a special agent with the FBI's Cellular Analysis Survey Team explained that the suspect could not have been at a particular residence at a specified time because his phone did not connect to the small cell located nearby. Dep. of David Magnuson 33-35, *State v. Roberts*, No. 13-009778CF10A (Fla. 17th Cir. Ct. May 3, 2016).

The future trajectory of the technology is also clear. As service providers roll out the next generation cellular network (5G), small cells will play an even greater role and will be deployed in significantly greater numbers, with marked effects on the precision of CSLI. *See* Tech. Experts Br. 16-17 & n.23. Femtocells, for example, have a broadcast radius of just 10 to 20 meters, meaning that CSLI is now able to place a phone in an area as much as five

times *smaller* than the oval plaza in front of the Supreme Court. *See* Joseph Hoy, *Forensic Radio Survey Techniques for Cell Site Analysis* 69 (2015) (discussing small cell broadcast coverage); *Hodge v. Talkin*, 799 F.3d 1145, 1151 (D.C. Cir. 2015) (dimensions of Court's plaza). Similarly, precise historical location estimates produced by service providers measuring the time and angle of signals arriving at their towers can be accurate to within 50 meters or less. Tech. Experts Br. 18.

2. Even on their own terms, this Court's cases involving "the third-party doctrine" do not apply here.

a. Contrary to the government's repeated claim (Resp. Br. 15-21, 28-29), the fact that a third party has access to information has never been sufficient, on its own, to divest the information of Fourth Amendment protection. Even in *Miller* and *Smith* themselves, this Court stressed the need to "examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents." *Miller*, 425 U.S. at 442; *accord Smith*, 442 U.S. at 741. Were exposure of information to a third party dispositive, those cases would have been much more easily decided. The Court need not have considered, for example, that pen registers have "limited capabilities," "disclos[ing] only the telephone numbers that have been dialed," and not "whether the call was even completed." *Smith*, 442 U.S. at 741-42.

The contrast here is dramatic. As petitioner has explained, weeks or months of CSLI can reveal extraordinarily intimate and sensitive information,

including, most significantly, one's detailed whereabouts over extended periods of time. *See supra* at 4-5; Petr. Br. 16-17. The government has never before been able to track anyone, much less everyone, in this way. And regardless of the particular details revealed in any given set of data, the mere "[a]wareness that the Government may be watching chills associational and expressive freedoms." *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring); *see also* Ctr. for Competitive Politics Br. 11-12; Elec. Privacy Info. Ctr. Br. 20 n.7; Reporters Comm. Br. 17-22.

b. Contrary to the government's claim (Resp. Br. 31), CSLI is not "voluntarily" conveyed within the meaning of *Miller* and *Smith*. Unlike a phone number entered into a phone to connect a call or a check passed into commerce to be drawn on an account, cell phone location data does not necessarily involve any voluntary act on the part of users. The data is created whenever mobile devices receive a call, text message, or data connection, requiring no activity of a user whatsoever. Moreover, the location data does not even directly relate to the functions the device performs. Unlike the phone number necessary to place the call or the negotiable instrument necessary to transfer funds, a person using a smartphone does not consciously share her geographic location with her service provider each time someone sends her an email or her phone automatically downloads an updated weather forecast.

Moreover, the many functions smartphones perform further distinguish this case from the discrete uses of landline telephones in *Smith* and

banking services in *Miller*. A smartphone is the nerve center used to organize and manage virtually every aspect of the user's personal (and often professional) life. *See Riley*, 134 S. Ct. at 2489; Tech. Cos. Br. 14-17; Data & Society Research Inst. Br.; Petr. Br. 39-42. Carrying a device so central to one's self-expression, well-being, safety, and livelihood is not "just as volitional as . . . exposing the numbers [one] dials" to a telephone service provider, Resp. Br. 32.

And while some users may be vaguely aware that their phones have to connect to cell towers, few if any are likely to know that every such connection is recorded and maintained, even when one turns off location services on one's phone. Unlike the banking and call records at issue in *Miller* and *Smith*, cellular subscribers do not receive records from their providers showing that this information has been collected. Thus, it is a fiction to claim that the information is in any meaningful sense voluntarily shared.

c. This case is also different from *Miller* and *Smith* because a federal statute (the Telecommunications Act) protects the privacy of the information here and gives further expression to the public's expectation of privacy. The government says that Section 222 of the Act similarly protected the information at issue in *Smith*, and so recognizing its relevance would require "overruling" that case. Resp. Br. 22. But the statute postdates *Smith* by 17 years, so it could not have played any role in the Court's analysis there. More important, Section 222 gives location records a level of explicit protection above

and beyond any other telecommunications data. *Compare* 47 U.S.C. § 222(c)(1), *with id.* § 222(f).

The government also argues that the particulars of Section 222 do not support any reasonable expectation of privacy and that, in any event, statutory protections are wholly irrelevant to the reasonable-expectation-of-privacy analysis. Resp. Br. 21-22. The government is wrong on both counts.

Under the Telecommunications Act, service providers may disclose cell phone location information only in limited circumstances: in aggregate, anonymized form without customer consent, 47 U.S.C. § 222(c)(3); in individually identifiable form only with the "express prior authorization" of the customer, *id.* § 222(c)(1), (f), or in an emergency, *id.* § 222(d)(4); and as otherwise "required by law," *id.* § 222(c)(1). Focusing exclusively on the last, vague provision, the government argues that the statute puts people on notice that CSLI can be lawfully obtained under the Stored Communications Act ("SCA") without a warrant. Resp. Br. 21-22, 42-43. But of course, any statutory commands must be read consistently with the Constitution. *Clark v. Martinez*, 543 U.S. 371, 381 (2005). Providing access "as required by law" only begs the question of what the Fourth Amendment requires. If, as petitioner argues, the Fourth Amendment requires a warrant, then any mechanism for warrantless access under the SCA falls away.

Moreover, the Fourth Amendment turns on "the everyday expectations of privacy that we all share" against incursions by members of the public at large. *Minnesota v. Olson*, 495 U.S. 91, 98-99

(1990). It is thus the explicit statutory protection against unconsented access to CSLI by other members of the public, rather than any special provision for law enforcement access, that reflects societal expectations of privacy. The government's reading of the provision permitting disclosure "as required by law" as carte blanche for police agencies is contrary to Congress's plain purpose and, more fundamentally, the Fourth Amendment.

d. Finally, the cases involving human eyewitnesses or informants do not govern here. *See* Resp. Br. 18, 35 (citing *Hoffa v. United States*, 385 U.S. 293 (1972), and *United States v. Jacobsen*, 466 U.S. 109 (1984)). It is a basic truth of human interactions that a person may, upon learning information, choose to share the contents of her mind with others. Hence, this Court has long held that a person assumes the risk that a confidant may divulge such information to others, including the authorities. *Hoffa*, 385 U.S. at 303. Here, by contrast, societal expectations and a federal statute prohibit service providers from sharing CSLI with the general public.

Jacobsen is similarly inapposite. There, employees of a private freight carrier observed an apparently illicit substance in a package and, without any government involvement, chose to inform the government of what they had seen. 466 U.S. at 111. The government then inspected the package, observing the incriminating information that had already been revealed through the private company's inspection. *Id.* Here, in contrast, no employee of MetroPCS or Sprint ever had reason to view petitioner's location records. The data was kept

in an automated system for billing and network diagnostic purposes, sight unseen. Only as a result of *law enforcement* action did the companies extract petitioner's data and provide it to the government, where it was for the first time examined.[1]

3. The government's complaint (Resp. Br. 30) that it would be "unworkable" in practice to hold that the third-party doctrine does not apply here is unpersuasive. A reasonable-expectation-of-privacy analysis must be grounded in "practical" realities. *Jones*, 565 U.S. at 963 (Alito, J., concurring in the judgment). Before the advent of CSLI and GPS technology, law enforcement could rarely, if ever, track a person's historical movements on a minute-by-minute basis for a period of time covering more than a few hours. *See* Petr. Br. 18-19, 31. Thus, if the government insists on specifying "how much is too much" when it comes to CSLI, a bright-line rule allowing law enforcement agents to request no more than 24 hours of an individual's historical CSLI without triggering the warrant requirement would give the government every benefit of the doubt in practical terms and the certainty it claims to need.

At the same time, it would be sufficient to resolve this case to hold that the one week's worth of CSLI the government requested from Sprint crosses the line, wherever exactly that line may be. Even if the Sprint order should be analyzed apart from the

---

[1] *Jacobsen* is especially irrelevant because, even if employees of the service providers *had* inspected petitioner's records and seen incriminating information, they would have been prohibited by statute from voluntarily "divulg[ing it] . . . to any governmental entity" absent an emergency. 18 U.S.C. § 2702(a)(3), (c)(4).

government's overall 152-day request, that order still allowed the government to obtain seven days of CSLI. Contrary to the government's contention (Resp. Br. 56-57), there is no practical or empirical basis for believing the government would typically have secured that amount of locational information before the advent of CSLI. And while the government cites a handful of cases recounting law enforcement surveillance, it offers no reason to believe they are anything other than outliers.

Moreover, only one of the cases the government cites actually involved anything close to longer-term, round-the-clock surveillance (although even there, it is impossible to tell from the opinion in the case the extent to which the suspect was continuously tailed). *United States v. Gramlich*, 551 F.2d 1359 (5th Cir. 1977). A second case involved surveillance only for limited time periods: Monday through Friday between 7:00 a.m. and 6:00 p.m. and Saturday from 7:00 a.m. to 1:00 p.m. Tr. of Proceedings at 299-300, *United States v. Caraballo*, No. 4:08-cr-35 (E.D. Va. Dec. 11, 2008), ECF No. 52, *aff'd* 384 F. App'x 285 (4th Cir. 2010). The government's other examples involved surveillance of one or more stationary locations—an exercise that is far less invasive and resource-intensive than tailing a suspect on the move. *See Young v. Owens*, 577 F. App'x 410, 412 (6th Cir. 2014) (store); *United States v. Gaskins*, 690 F.3d 569, 574 (D.C. Cir. 2012) (multiple locations) *United States v. Johnson*, 480 F. App'x 835, 837 (6th Cir. 2012) (residence); *Shades Ridge Holding Co. v. CIR*, 23 T.C.M. (CCH) 1665 (1964) (home).

In the end, the government's examples simply reinforce the concurring Justices' conclusion in *Jones* that it is extremely rare for law enforcement to tail a suspect for any significant period. *See Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment). And in this case, where police developed suspicion about petitioner only *after* the fact, and then sought to go back in time and recreate his past locations and movements over several months, the ability to gather location data has traditionally been even more constrained.

B. Procuring CSLI Intrudes on People's "Papers" Under the Fourth Amendment.

Neither of the government's responses to petitioner's property-based argument that a search occurred here withstands scrutiny.

1. Contrary to the government's assertion, Resp. Br. 41, petitioner's property-based argument is properly presented. The property-based rationale is an alternative argument supporting petitioner's legal claim that the government's acquisition of CSLI constitutes a search. "[O]nce a federal claim is properly presented, a party can make any argument in support of that claim; parties are not limited to the precise arguments they made below." *Lebron v. Nat'l R.R. Passenger Corp.*, 513 U.S. 374, 379 (1995). In any event, this Court may consider any argument that was "passed upon" by the court below. *United States v. Williams*, 504 U.S. 36, 41 (1992). The Sixth Circuit addressed this argument, holding that "[t]he

defendants of course lack any property interest in [the] cell-site records." Pet. App. 12a.[2]

2. On the merits, the government argues that the Telecommunications Act cannot create a proprietary interest in CSLI because it provides exceptions to its nondisclosure rule. Resp. Br. 42. But as petitioner has explained, the statute creates a property interest because it provides cell phone users with the rights to exclude others from their CSLI and to limit its use. Petr. Br. 33-34. That the service provider retains possession of, and a limited right to use, the records does not alter this conclusion. A person need not possess *all* of the "bundle of sticks" of property rights in order to have a protected interest in a location or thing. *See Dickman v. C.I.R.*, 465 U.S. 330, 336 (1984). That is why the Federal Communication Commission has concluded –in a determination the government never mentions, much less refutes –that papers containing CSLI are *customers'* records. Petr. Br. 33-34.

---

[2] The government also incorrectly asserts that the parties' joint stipulation that the CSLI records "are authentic and accurate business records of the[service providers]," JA 51, precludes petitioner's argument here. Resp. Br. 18, 41-42. That stipulation simply allowed the government to avoid calling employees of the companies to testify to their recordkeeping practices. *See* Fed. R. Evid. 803(6) (exception to hearsay rule for certain records kept by businesses). It was not a substantive determination about petitioner's privacy or property interest.

C. The Government's Theory Would Negate Fourth Amendment Protection For A Wide Range Of Vital Privacy Interests In The Digital Age.

Attempting to reassure the Court that its proposed rule won't sweep too far, the government suggests that the contents of electronic communications and other digital information might be exempted from the third-party doctrine. Resp. Br. 36-38. While the contents of emails and other digital-age communications are surely protected by the Fourth Amendment, the government provides an unconvincing account of how they can be distinguished from the records at issue here.

1. The government posits a distinction between information "communicated *to* the providers" and information that "merely passes *through* their communications networks, with no general right of the provider to use or control the contents." Resp. Br. 36-37. That may provide a clean distinction for physical letters, which remain sealed in transit, *see Ex Parte Jackson*, 96 U.S. 727, 733 (1877), but it fails to accurately reflect the way emails are handled.

In fact, service providers *do* retain the right to access the contents of emails. As the government has recently explained elsewhere, "the terms of service currently applicable to Microsoft's free email service do not suggest a mere caretaker or trust relationship. Rather, they assert Microsoft's right to access or use the *contents* of its customers' emails." Br. for the U.S., *Microsoft v. United States*, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985), 2015 WL 1139654, at *41,

cert. granted, No. 17-2 (Oct. 16, 2017). Other major email service providers also access the contents of emails to provide "customized search results, tailored advertising, and spam and malware detection," among other purposes. Google Terms of Service, https://www.google.com/policies/terms; *see also* Final Reply Br. for Def.-Appellant U.S., *Warshak v. United States*, 532 F.3d 521 (6th Cir. 2008) (No. 06-4092), 2007 WL 2085416 ("Yahoo! has access to and control over the e-mail stored on its servers.").

Thus, if the content of email is protected by the Fourth Amendment, it is not because of how email is transmitted or exposed to service providers. Rather, it is because of the strong expectation of privacy in email notwithstanding providers' access. CSLI should be protected for the same reason. Just as people have never expected the government to have free access to the contents of their private communications merely because they are transmitted through third parties, they have never expected that the government would be able to obtain a pervasive record of their past locations and movements upon request.

2. Email is just the beginning. As the Technology Companies explain, "all digital technology transmits user information to various service providers[, and t]hose transmissions are an unavoidable condition of using digital technology." Tech. Cos. Br. 18. Much of this information is *provided to* rather than *transmitted through* third parties. Thus, under the government's theory, such information would be available to the government without any Fourth Amendment protections—including "health and fitness data" from a

smartphone app or smartwatch, information about "a homeowner's habits" from internet-of-things devices in the home, and the entire record of what a person searches, browses, or reads online. *Id.* at 18-19; Petr. Br. 44-47.

II. WARRANTLESS SEARCH OF LONGER-TERM HISTORICAL CSLI IS UNREASONABLE UNDER THE FOURTH AMENDMENT.

If this Court reaches the issue, it should hold that a warrant is required to conduct a search of CSLI. None of the government's arguments to the contrary has merit.

A. The Subpoena Power Does Not Allow The Government To Obtain Records Held By A Third Party In Which There Is A Reasonable Expectation Of Privacy.

The government does not contest that this Court's opinions upholding use of subpoenas to obtain records from third parties have never addressed a situation in which the subject of the investigation has a reasonable expectation of privacy or property interest in the records. The government attempts to explain this away by asserting that it "is because the Court applied the third-party doctrine" in those cases. Resp. Br. 47 n.12. But that is a perfectly circular explanation. If records in a third party's possession do implicate a subject's reasonable expectation of privacy, a subpoena is not sufficient to satisfy the Fourth Amendment.

First-party subpoenas generally satisfy the Fourth Amendment for two reasons: (1) they are less intrusive than a typical search, because the subject himself produces the material; and (2) they permit the subject to challenge the subpoena before his privacy is invaded. *See Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 414-15 (1984); Resp. Br. 45. Neither rationale applies where, as here, a subpoena seeks information from a third party in which the subject has a reasonable expectation of privacy. In that context, (1) a subpoena is just as intrusive of the subject's privacy as any full-scale search of the third party would be; and (2) the subject has no pre-enforcement opportunity to challenge the subpoena, as he lacks notice.

None of the government's fallback arguments hold water either.

1. The government first (and most dramatically) seeks a categorical rule of form over substance, asking the Court to hold that once investigators have chosen to proceed via subpoena, that choice should be upheld without regard to the expectation of privacy in the information sought. Resp. Br. 47. Not surprisingly, that cannot be squared with this Court's analysis in third-party subpoena cases. In those cases, the Court has carefully assessed whether the subject of the investigation has a reasonable expectation of privacy in the records requested. *See, e.g.*, *Miller*, 425 U.S. at 442; *Couch v. United States*, 409 U.S. 332, 336 (1973); *see also Fisher v. United States*, 425 U.S. 391, 399, 401 n.6 (1976). The only coherent reason for doing so is that, where such expectation exists, it renders the subpoena unreasonable.

Indeed, the government's theory countenances *no* type of record or information for which criminal investigators would be required to seek a warrant: not the data from a suspect's phone stored in the cloud, *but see Riley*, 134 S. Ct. at 2491, or the contents of her emails held by a provider, *but see United States v. Warshak*, 631 F.3d 266, 285-88 (6th Cir. 2010).

It is no answer to say, as the government does, that "the subpoena standard itself" can "impose more stringent requirements depending on the nature of the requested documents." Resp. Br. 48. Under this approach, magistrates would have to decide when information poses "[s]pecial problems of privacy" and draw distinctions between "relevance" and "unquestionable relevance." *Id.* (alteration in original and citation omitted). It would be far clearer to enforce the familiar warrant requirement than to require magistrates to apply such novel and amorphous tools to manage governmental requests to conduct searches.

Moreover, the government misreads even the case on which it relies for its suggested enlargement of the subpoena power. *Id.* In *Fisher v. United States*, taxpayers and attorneys challenging summonses for tax preparation materials did not raise Fourth Amendment arguments. 425 U.S. at 401 n.7. In dicta, the Court noted that any such argument would fail because the request at issue *itself* sought "only documents of unquestionable relevance." *Id.* The Court then went on to explain that "[s]pecial problems of privacy which might be presented by subpoena of a personal diary are not involved here." *Id.* (citation omitted). The implication is that even an

"unquestionabl[y] relevant" subpoena could not compel production of something as private as a diary entrusted to the care of another.

2. The government next argues that requiring a warrant here "would impede longstanding investigatory practices" involving subpoenas. Resp. Br. 49. But requiring a warrant for CSLI will leave the government's compulsory process power intact in the vast majority of cases. A warrant requirement here will have no bearing, for example, on administrative subpoenas issued in regulatory investigations, where the special-needs exception applies. *See v. City of Seattle*, 387 U.S. 541, 544-45 (1967). It will likewise not impede use of criminal investigative subpoenas in the multitude of cases where the government seeks corporate books, tax records, or other documents in which courts have held that no person has a reasonable expectation of privacy. *See, e.g.*, *Couch*, 409 U.S. at 336 & n.19.

3. The government lastly maintains that the lack of notice that flows from using its subpoena power is acceptable because contemporaneous notice is not required for warrants either. But in the context of records held by third parties in which a reasonable expectation of privacy exists, the requirement of a warrant is a *substitute* for the right to pre-enforcement challenge that would otherwise accompany a first-party subpoena. Warrants, which issue upon probable cause, supported by oath or affirmation, and describe with particularity the scope of the search, provide critical procedural and substantive safeguards when the investigative target cannot advance her own rights.

The government responds that the service provider can object before producing records. Resp. Br. 45. But service providers will generally lack the incentive or knowledge to raise their subscribers' Fourth Amendment interests. And even when providers have done so in other cases, the government has argued that they lack such authority. *See* Mot. To Dismiss 10, *Microsoft v. U.S. Dep't of Justice*, 233 F. Supp. 3d 887 (W.D. Wash. 2017) (No. C16-0638), 2016 WL 4120319 (citing *Alderman v. United States*, 394 U.S. 165, 174 (1969)). In the absence of notice, only a warrant can safeguard the populace's Fourth Amendment rights.

B. Principles Of Fourth Amendment Reasonableness Require A Warrant.

As a last resort, the government invites this Court to assess the legitimacy of the search here through a general balancing of interests. Resp. Br. 50. But the only authority the government cites in this respect is *Maryland v. King*, in which this Court applied the "special needs" doctrine to uphold limited searches of a category of people—arrestees—with diminished expectations of privacy. 133 S. Ct. 1958, 1969-70, 1978 (2013). That *King* does not apply here is reason enough to reject the government's argument. *See* Petr. Br. 49. At any rate, a balancing of interests confirms that conducting a warrantless search of longer-term historical CSLI is unreasonable.

1. On one side of the balance, the privacy interest in not having the government know where one has traveled minute-by-minute over extended periods is high. And absent any constitutional check, Section 2703(d) does not prevent police from

obtaining huge swaths of CSLI—more than a year's worth in some cases—thus exposing large volumes of private information to government scrutiny. *See, e.g.*, *United States v. Brown*, 2017 WL 4216979, at *5 (D. Neb. 2017) (454, 388, and 186 days of suspects' CSLI). Only the probable cause and particularity requirements of a warrant can provide appropriate protection.

2. On the other side of the balance, the government lacks a sufficiently compelling interest to overcome the presumptive requirement of a warrant.

The government asserts an interest in accessing CSLI "during the early stages of an investigation, when the police [may] lack probable cause." Resp. Br. 51 (alteration in original). But that argument can be advanced about *every* search. In *Jones*, for example, the government asserted the same "interest of law enforcement in investigating leads and tips . . . before those suspicions have ripened into probable cause." U.S. Reply Br. 22, *Jones* (No. 10-1259). This Court rejected the argument and should do so again here. Under petitioner's rule, as under the concurring opinions in *Jones*, the government may obtain shorter-term locational information without a warrant. That generally satisfies any legitimate interest in collecting evidence early in an investigation, before the government has developed probable cause. *See* Resp. Br. 52 (citing cases where the government obtained, or could have obtained, short-term CSLI); State AGs Br. 20-22 (same).

Further, in the mine-run of cases, the government likely already has probable cause when it applies for a 2703(d) order, as demonstrated by the

facts set out in the applications in numerous cases. *See, e.g.*, *Ford v. State*, 477 S.W.3d 321, 325 (Tex. Crim. App. 2015) (finding that the application under § 2703(d) actually established probable cause). A warrant requirement will impose no undue burden.

C. Congressional Inaction Is Irrelevant Here.

Petitioner has already explained why the SCA does not represent "a judgment by Congress" as to how to appropriately protect historical CSLI, Resp. Br. 53. Congress did not contemplate the existence of historical CSLI, let alone its future ubiquity, when crafting the statute. Petr. Br. 49-50.

The government argues that Congress has since considered and declined to enact various amendments to the SCA that would have addressed CSLI more directly. Resp. Br. 54-55. But as this Court has repeatedly explained, "[c]ongressional inaction lacks persuasive significance because several equally tenable inferences may be drawn from such inaction." *Pension Ben. Guar. Corp. v. LTV Corp.*, 496 U.S. 633, 650 (1990) (internal quotation marks omitted). That is especially the case here, where legislative chokepoints have stymied overwhelmingly popular attempts to update the SCA. *See, e.g.*, Email Privacy Act, H.R. 699, 114th Cong. (2015) (passed by House on unanimous vote, but unable to receive vote in Senate).

Absent meaningful legislative action, the task once again falls on this Court to enforce the requirements of the Fourth Amendment. It should do so here to preserve the reasonable expectation of

privacy that Americans have long enjoyed in the details of their location over a long period.

CONCLUSION

For the foregoing reasons, the judgment of the Sixth Circuit should be reversed.

Respectfully submitted,

Nathan Freed Wessler
Ben Wizner
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004

David D. Cole
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
915 15th Street, NW
Washington, D.C. 20005

Cecillia D. Wang
Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111

Harold Gurewitz
Counsel of Record
GUREWITZ & RABEN, PLC
333 W. Fort Street, Suite 1400
Detroit, MI 48226
(313) 628-4733
hgurewitz@grplc.com

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
AMERICAN CIVIL LIBERTIES UNION FUND OF MICHIGAN
2966 Woodward Ave.
Detroit, MI 48201

Jeffrey L. Fisher
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305

Dated: October 24, 2017

RECORD AND BRIEFS

Supreme Court, U.S.
FILED
SEP 2 - 2017
OFFICE OF THE CLERK

No. 16-402

In the Supreme Court of the United States

TIMOTHY IVORY CARPENTER,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

ON WRIT OF CERTIORARI TO THE
UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

BRIEF FOR THE STATES OF ALABAMA, ARIZONA, COLORADO, FLORIDA, IDAHO, INDIANA, KANSAS, KENTUCKY, MARYLAND, MICHIGAN, MONTANA, NEBRASKA, NEW HAMPSHIRE, NEW MEXICO, OKLAHOMA, PENNSYLVANIA, SOUTH CAROLINA, TENNESSEE, AND WYOMING AS AMICI CURIAE IN SUPPORT OF RESPONDENT

Office of the Attorney General
PL-01, The Capitol
Tallahassee, Florida 32399
Amit.Agarwal@myfloridalegal.com
(850) 414-3300

PAMELA JO BONDI
Attorney General of Florida

AMIT AGARWAL
Solicitor General
**Counsel of Record*
DENISE M. HARLE
JORDAN E. PRATT
Deputy Solicitors General

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

INTEREST OF AMICI STATES 1

SUMMARY OF THE ARGUMENT 2

ARGUMENT 7

I. The Government Does Not "Search" a Phone User When a Neutral and Detached Magistrate Orders a Third-Party Phone Company to Disclose Its Own Cell-Tower Records Pursuant to the Privacy-Protecting Provisions of the SCA 7

A. Petitioner may not assert a constitutionally cognizable privacy interest in historical cell-tower records made, kept, and owned by a third-party service provider. 7

B. Fourth Amendment jurisprudence should not encourage the use of new technologies as instrumentalities of crime. 12

C. This Court's third-party doctrine need not be construed to defeat more substantial expectations of privacy not at issue in this case 14

II. The Challenged SCA Orders Were Constitutionally Reasonable. 16

A. The warrant procedure should not be mechanically applied to congressionally-authorized "searches" arising out of the issuance of compulsory process for third-party cell-tower records. 16

B. As real-world examples make clear, Section 2703(d) orders for cell-tower records serve compelling governmental interests, at little or no cost to individual privacy. 19

C. Congress and the state legislatures should be free to craft reasonable legislative solutions to the difficult problems arising out of compulsory disclosure of third-party records. 25

D. Reasonable considerations support the application for longer-term records in cases like this one. 31

III. Section 2703(d) Is Not Unconstitutional in All Its Applications to Cell-Tower Records. 34

CONCLUSION 36

TABLE OF AUTHORITIES

Cases

Couch v. United States,
409 U.S. 322 (1973) 11

Donaldson v. United States,
400 U.S. 517 (1971) 12

In re Application of the United States for Historical Cell Site Data,
724 F.3d 600 (5th Cir. 2013) 10, 26

Kentucky v. King,
131 S. Ct. 1849 (2011) 17

Kyllo v. United States,
533 U.S. 27 (2001) 3, 13

McMann v. Sec. & Exch. Comm'n,
87 F.2d 377 (2d Cir. 1937) 24

Nw. Austin Mun. Utility Dist. No. One v. Holder,
557 U.S. 193 (2009) 20

Okla. Press Pub. Co. v. Walling,
327 U.S. 186 (1946) 5, 18

Rawlings v. Kentucky,
448 U.S. 98 (1980) 8

Riley v. California,
134 S. Ct. 2473 (2014) 25

Sec. & Exch. Comm'n v. Jerry T. O'Brien, Inc.,
467 U.S. 735 (1984) 11

Smith v. Maryland,
442 U.S. 735 (1979) ..... passim

United States v. Carpenter,
819 F.3d 880 (6th Cir. 2016) 13, 19, 32

United States v. Davis,
785 F.3d 498 (11th Cir. 2015) (en banc) ..... passim

United States v. Graham,
846 F. Supp. 2d 384 (D. Md. 2012) 11, 14

United States v. Jones,
565 U.S. 400 (2012) 27, 36

United States v. Karo,
468 U.S. 705 (1984) 18, 36

United States v. Knotts,
460 U.S. 276 (1983) 16, 36

United States v. Miller,
425 U.S. 435 (1976) ..... passim

United States v. Nixon,
418 U.S. 683 (1974) 26

United States v. Oreckinto,
2017 WL 131563 (D. Conn. Jan. 13, 2017) 23

United States v. Oreckinto,
2017 WL 1371255 (D. Conn. Apr. 14, 2017) 23

United States v. Oreckinto,
234 F. Supp. 3d 360 (D. Conn. 2017) 23

United States v. R. Enters.,
498 U.S. 292 (1991) 24

United States v. Warshack,
631 F.3d 266 (6th Cir. 2010) 15

United States v. Watson,
423 U.S. 411 (1976) 19

Wash. State Grange v. Wash. State Republican Party,
552 U.S. 442 (2008) 35

Wyoming v. Houghton,
526 U.S. 295 (1999) 18

Statutes

18 U.S.C. §2702(c) 16

18 U.S.C. §2703(c)(1)(B) 1

18 U.S.C. §2703(d) ..... passim

2014 Md. Laws Ch. 191 28

725 Ill. Comp. Stat. 168/10 30

Cal. Penal Code §1546.1(e) 31

Cal. Penal Code §1546.1(g) 31

Cal. Penal Code. §1546.1(d)(2) 30

Colo. Rev. Stat. §16-3-303.5(1)(d) 28

Conn. Gen. Stat. §54-47aa 31

Conn. Stat. §54-47aa 28

La. Rev. Stat. §844.9B.(4)–(5) 30

Md. Code Ann. Crim. §1-203.1(d) 31

Me. Rev. Stat. tit. 16 §649 31

Minn. Stat. §626A.42 28

Minn. Stat. §626A.42(1)(e) 28

N.H. Rev. Stat. Ann. §644-A 28

N.H. Rev. Stat. Ann. §644-A:61.V 28

R.I. Gen. Laws §12-32-3 31

Utah Code Ann. §77-22-2.5(2) 30

Utah Code Ann. §77-23c-102(1)(a) 30

Utah Code Ann. §77-23c-102(1)(b) 30

Utah Code Ann. §77-23c-102(1)(d) 31

Va. Code Ann. § 19.2-70.3(E) 30

Va. Code Ann. §19.2-70.3(B) 29

Vt. Stat. Ann. tit. 13, §8102(g) 31

Vt. Stat. Ann. tit. 13, §8103 31

Vt. Stat. tit. 12, §8102(f) 16

Other Authorities

En Banc Brief for the United States, *United States v. Davis* (11th Cir. 2014) (No. 12-12928), 2014 WL 7232613 9

Filings of Defendant, United States v. Carpenter, No. 12-cr-20218 (E.D. Mich.) 8, 34

Subpoena, XVII Oxford English Dictionary 50 (2d ed. 1989) 13

Constitutional Provisions

U.S. CONST. amend. IV 7

INTEREST OF *AMICI* STATES

Amici are the States of Alabama, Arizona, Colorado, Florida, Idaho, Indiana, Kansas, Kentucky, Maryland, Michigan, Montana, Nebraska, New Hampshire, New Mexico, Oklahoma, Pennsylvania, South Carolina, Tennessee, and Wyoming.[1]

This case involves a challenge to the constitutionality of a statute authorizing a "governmental entity" to apply for a non-warrant court order compelling third-party telephone-service providers to produce historical cell-tower records that are "relevant and material to an ongoing criminal investigation." *See* 18 U.S.C. §2703(c)(1)(B), (d). State law-enforcement authorities rely heavily on such orders, which may be sought by state prosecutors and issued by state judges, *id.* §§2703(c)(1)(B), (d), 2711(3)(B), (4), and which "are routinely used to investigate the full gamut of state and federal crimes, including child abductions, bombings, kidnappings, murders, robberies, sex offenses, and terrorism-related offenses." *United States v. Davis*, 785 F.3d 498, 518 (11th Cir. 2015) (en banc). Accordingly, *amici* states have a substantial interest in the Court's disposition of this case.

---

[1] No counsel for any party authored this brief, in whole or in part, and no person or entity other than amici contributed monetarily to its preparation or submission. The parties lodged blanket consents with the Clerk.

SUMMARY OF THE ARGUMENT

I. No "search" of which Petitioner has standing to complain took place when two telephone companies produced their own routing-related records to the government.

A. The Fourth Amendment protects "[t]he right of the people to be secure in *their* . . . papers," not in the papers of *others*. Nevertheless, Petitioner asks this Court to hold that he has a constitutionally cognizable privacy interest in business records that he did not make or own and has never seen or kept, and that contain information he voluntarily conveyed to a third party. That claim fails on its own terms, and it cannot be reconciled with the principles enunciated in this Court's prior cases. Indeed, Petitioner's claim is substantially weaker than the claims this Court rejected in *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976).

B. Petitioner's use of a cell phone does not give him a Fourth Amendment right to conceal information that otherwise would not have been private. A cell site is a cell *tower*, not the site of a cell *phone*. The "cell-site" records Petitioner sought to suppress identify the cell towers used to connect incoming and outgoing calls. Before cell phones were in use, such calls had to be routed via landline telephones tied to fixed and readily identifiable locations; and calls using such phones would have generated third-party records revealing much more specific location-related data than the general vicinity information circumstantially discernible from cell-tower records. That was the case in *Smith*, which approved the acquisition of pen-register data tending

to place petitioner inside a constitutionally protected place—his own home. *See* 442 U.S. at 737.

In other words, the Fourth Amendment should not "permit police technology to erode the privacy guaranteed by the Fourth Amendment," *Kyllo v. United States*, 533 U.S. 27, 34 (2001); but it also should not permit private technologies to be used with impunity as instrumentalities of crime—i.e., to conceal information that could not have been shielded from the ordinary truth-seeking tools of the judicial system if older technologies had been used to engage in the same underlying conduct.

C. There is nothing troubling about applying the third-party doctrine to uphold the congressionally regulated and judicially supervised investigative tool at issue here. Under the statutory provision Petitioner asks this Court to strike down, a phone company may not be required to disclose any of its cell-tower data unless and until all three branches of the government acquiesce in the disclosure. That statutory procedure does not *lower* the bar from a warrant to a non-warrant order; it *raises* the bar from an ordinary subpoena to one that incorporates a broad range of additional privacy protections. *Davis*, 785 F.3d at 505–06.

Future cases, which may involve more sensitive data obtained without the safeguards of the Stored Communications Act (SCA), might well raise distinct concerns. Accordingly, this Court should exercise caution in articulating the contours of the third-party doctrine. As the federal Courts of Appeals have recognized, that doctrine need not be construed to defeat

more substantial privacy concerns that are not implicated by compulsory process for the disclosure of cell-tower records under the SCA.

II. Any "search" of Petitioner arguably arising out of a third-party phone company's production to the government of its own records was not "unreasonable" within the meaning of the Fourth Amendment.

A. The Fourth Amendment bars *unreasonable* searches, not *warrantless* searches. The "warrantless" issuance of a court order under §2703(d) does not make that order unreasonable, for three reasons.

1. The SCA goes above and beyond well-established constitutional prerequisites governing the issuance of compulsory process. That settled law does not require the government to get a warrant before a judicial subpoena may issue; and a Section 2703(d) order is, at bottom, a judicial subpoena, albeit one that incorporates additional privacy protections. In any event, the SCA effectuates the "primary purpose" of the warrant procedure—the interposition of a neutral and detached magistrate between law-enforcement officers and the evidence they seek.

2. A traditional Fourth Amendment analysis supports the reasonableness of the challenged court orders. It is no answer to say that the "warrant requirement" already "strikes the appropriate balance" (Pet. Br. 53–54). As applied to compulsory process, this Court's cases hold that requirements "literally applicable in the case of a warrant" are "satisfied" by a *different* reasonableness test. *See Okla. Press Pub. Co. v. Walling*, 327 U.S. 186, 209 (1946). The SCA passes

that test, and Petitioner does not try to argue otherwise. Petitioner may ask this Court to carve out a new exception to that longstanding law; but he should bear the burden of showing that a traditional balancing of interests supports any such doctrinal innovation.

3. A "strong presumption of constitutionality" applies to congressionally-authorized searches. That "strong presumption" should weigh at least as heavily as the ordinary default rule in favor of warrants. And it should apply with particular force to a "search" based on the *Katz* test, since Congress is especially well-positioned to assess contemporary expectations of privacy and to balance those expectations against competing societal interests.

B. As real-world examples illustrate, SCA orders for cell-tower records serve compelling governmental interests—exonerating the innocent, apprehending the guilty, and protecting the public. When obtained pursuant to the privacy-protecting provisions of the SCA, those real-world benefits come at a negligible cost to individual privacy.

C. There is no "simple answer" to the complicated and difficult question of social policy Congress sought to resolve in enacting the SCA. The answer Congress provided—to break up the pertinent investigative power, allocate it among the three branches of government, and require unanimous interbranch cooperation *before* the government may compel a third party to produce any potentially sensitive evidence in its possession—embodies a particularly enlightened and elegant solution. Like the SCA, state legislative enactments protecting location-related information support

the conclusion that the people's elected representatives are up to the task of assessing contemporary expectations of privacy and carefully balancing those expectations against competing societal interests.

D. In cases like this one, reasonable considerations support the application for "longer-term" cell-tower records. Such records help investigators and prosecutors (at the front end) and juries and judges (at the back end) to make sense of the general vicinity information circumstantially discernible from "shorter-term" cell-tower records; and that is the case precisely because, as defendants frequently emphasize, cell-tower records do not disclose the identity or precise location of a phone user. Petitioner is not in a good position to urge otherwise; in the district court, he faulted the government for analyzing *too little*—and not *too much*—cell-tower data. At any rate, it was reasonable for the government to seek four months of cell-tower records when, as here, "specific and articulable facts" established "reasonable grounds to believe" that Petitioner had committed four months of robberies.

III. Assuming *arguendo* that the government violated the Fourth Amendment when it obtained "longer-term" cell-tower records for a phone tied to Petitioner, Section 2703(d) is not unconstitutional in all its applications to cell-tower records. Settled law compels the conclusion that the government may obtain "shorter term" cell-tower data to determine whether a particular phone was in the vicinity of a public crime scene, particularly when such information is obtained from a third party pursuant to a court order authorized by Congress in a privacy-protecting statute.

ARGUMENT

I. THE GOVERNMENT DOES NOT "SEARCH" A PHONE USER WHEN A NEUTRAL AND DETACHED MAGISTRATE ORDERS A THIRD-PARTY PHONE COMPANY TO DISCLOSE ITS OWN CELL-TOWER RECORDS PURSUANT TO THE PRIVACY-PROTECTING PROVISIONS OF THE SCA.

A. Petitioner may not assert a constitutionally cognizable privacy interest in historical cell-tower records made, kept, and owned by a third-party service provider.

The Fourth Amendment protects "[t]he right of the people to be secure in *their* papers," not in the papers of *others*. U.S. CONST. amend. IV (emphasis added). Consistent with the constitutional text, "[t]his Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him [i.e., the third party] to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *United States v. Miller*, 425 U.S. 435, 443 (1976); *see Smith v. Maryland*, 442 U.S. 735 (1979).

The logic of those cases applies here. *See* U.S. Br. 15–36. Indeed, Petitioner's claim is substantially weaker than the claims this Court rejected in *Smith* and *Miller*, for several reasons.

First, and as a threshold matter, Petitioner did not meet his burden of establishing Fourth-Amendment standing to challenge the records he sought to

suppress. *See Rawlings v. Kentucky*, 448 U.S. 98, 104–05 (1980). The records here at issue pertain to a phone registered under the name "Michael Mayers." Pet. App. 76a. In his motion to suppress, Petitioner never acknowledged that the phone in question was his, or that he was using it at the relevant times. *See Filings of Defendant, United States v. Carpenter*, No. 12-cr-20218 (E.D. Mich.), ECF Nos. 196, 214, 216, 223; *Transcript of Jury Trial*, ECF No. 326, at 155–61. To the contrary, he argued (incorrectly) that the government's application for a court order under §2703(d) "provide[d] no connection between the allegations of the investigation and individuals named in the application, Timothy Sanders and Timothy Carpenter." *Id.* ECF No. 223, at 3; No. 326, at 159; *see also id.* ECF No. 333, at 71 (asserting, in closing argument to the jury, that the agent who testified about cell-tower records "really just talked to you about numbers on cell phones and where he saw the calls made," and didn't "have any direct information about Timothy Carpenter").

Those omissions matter. Modern-day criminals frequently obtain disposable burner phones that may be registered under fictitious aliases and used as instrumentalities of crime.[2] That trend significantly

---

[2] In *Davis*, for example, the defendant used a MetroPCS phone "registered to 'Lil Wayne.'" 785 F.3d at 503. That company—the same company whose service Petitioner used—did "not require[] the subscriber . . . to give his true name," and offered pay-as-you-go plans allowing easy cancellation of service. *See id.* at 503 n.5. Davis never admitted that he owned or possessed the phone in question. At trial, defense counsel emphasized that the government's cell-tower expert did not know whether the phone in

hampers law-enforcement investigations. And it makes it all the more important for the courts to enforce traditional rules governing the assertion of Fourth Amendment standing.

In other words, Petitioner had the option of distancing himself from the phone that was registered under the name "Michael Mayers"; and he could also have tried to assert a reasonable expectation of privacy in third-party records pertaining to that phone. But he did not have the right to do both at the same time.

Second, service contracts and privacy policies typically warn cell-phone customers that phone companies collect location-related information and may disclose such data to law-enforcement authorities. *See In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600, 613 (5th Cir. 2013). For example, MetroPCS's current privacy policy, which is accessible from the company's website, advises its wireless customers that the company "may disclose, without your consent, the approximate location of a wireless device to a governmental entity or law enforcement authority when we are served with lawful process." Similarly, the company warns that its "systems capture details about the . . . location of wireless device(s) you use"; that it "use[s] location information

---

question belonged to his client. The expert's cell-tower maps, defense counsel argued, would have indicated that the phone belonged to "Mickey Mouse" if the agent had been "told to do that" by the prosecutor. *See* En Banc Brief for the United States, *United States v. Davis* (11th Cir. 2014) (No. 12-12928), 2014 WL 7232613, at **9–11.

to route wireless communications and to provide 911 service, which allows emergency services to locate your general location"; and that it "allow[s] third parties the capability of accessing data about your location that is derived from our network."[3] *See also Smith*, 442 U.S. at 742–43 (considering publicly available information included in phone books and other sources in assessing whether Smith had an expectation of privacy in pen-register records). Such express warnings and contractual provisions, even if not dispositive, at least undermine Petitioner's assertion that he actually manifested an objectively reasonable expectation of privacy in MetroPCS's routing-related records.

Third, the Court in *Miller* held that a customer did not have a reasonable expectation of privacy in certain records made and kept by his bank, even though the bank was required by law to maintain those records. *See Miller*, 425 U.S. at 436, 441. In contrast, "[f]ederal law does not mandate that cellular providers create or maintain [historical cell tower] data," *United States v. Graham*, 846 F. Supp. 2d 384, 398 & n.11 (D. Md. 2012) (citing 47 C.F.R. 42.6). Hence, Petitioner's claim is "substantially weaker" than the claim the Court rejected in *Miller*. *See Sec. & Exch. Comm'n v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 n.11 (1984).

Arguments to the contrary are not persuasive.

1. Petitioner may not make out a right to be secure in someone else's "papers," *see* U.S. Const. amend. IV,

---

[3] MetroPCS Privacy Policy, *available at:* https://www.metropcs.com/terms-conditions/privacy.html (last visited October 2, 2017).

by asserting that those papers contained "his location data." Evidence lawfully in the possession of a third party is not *his*, even if it has to do with *him*. Indeed, the Fourth Amendment would not shield Petitioner from incriminating information in records turned over by a third party even if they were his. *See, e.g., Couch v. United States*, 409 U.S. 322, 324, 335–36 (1973) (holding that petitioner could not reasonably claim a Fourth Amendment expectation of privacy in records in which she "retained title" after she had "surrendered possession of the records" to her accountant).

2. As Respondent explains, Petitioner voluntarily conveyed the general vicinity information discernible from cell-tower records. U.S. Br. 21, 23–32. Properly understood, however, such voluntary conveyance is a sufficient—not a necessary—condition for the application of the third-party doctrine. For example, Petitioner did nothing to "convey"—and he may not even have known—the phone numbers of accomplices who called him (*see* J.A. 136). Regardless, he had no right to bar a third party from producing such non-privileged evidence to the government in compliance with a court order authorized by statute, even though that record supplies evidence of associations he might prefer to keep private. Similarly, it does not matter whether Petitioner meaningfully consented to the disclosure of the company's cell-tower records. Like the security-surveillance tapes introduced into evidence at his trial, such evidence was not his to withhold. *See Donaldson v. United States*, 400 U.S. 517, 545 (1971) (Douglas, J., concurring) ("There is no right to be free from incrimination by the records or testimony of others.").

3. This case does not involve governmental "surveillance" or "monitoring" of any kind. Under the SCA, law-enforcement officers do not and may not seek historical cell-tower records to spy on citizens or keep track of their comings and goings. Instead, they consult such records to help resolve questions of historical fact "relevant and material to an ongoing criminal investigation," §2703(d)—in this case, for example, whether Petitioner really was, as accomplices testified, close to the sites of various armed robberies at the times in question. For purposes of that inquiry, the phone company stands in the same shoes as any other witness lawfully in possession of non-privileged evidence relevant to an ongoing criminal investigation. The government does not engage in "surveillance" or "monitoring" when a court compels the production of preexisting documentary (or testimonial) evidence from such a witness, just as a grand jury does not "track" a suspect's movements when it issues a subpoena for a third-party business's security-surveillance videos to find out if a suspect was at the scene of a crime.

B. Fourth Amendment jurisprudence should not encourage the use of new technologies as instrumentalities of crime.

1. This case does not involve governmental use of a "new technology," Pet. Br. 15. Rather, the only tool the government used in this case—i.e., compulsory process for the production of preexisting evidence—is older than the Constitution itself. *See* Subpoena, XVII Oxford English Dictionary 50 (2d ed. 1989) ("He woll not come withoute he have a suppena.") (quoting letter

written in 1467). In 1768, for example, William Blackstone explained that books and papers "in the hands of third persons" "can generally be obtained by rule of court, or by adding a clause of requisition to the writ of *subpoena*, which is then called a *subpoena duces tecum*." *Id.* (quoting 1768 edition of the *Commentaries on the Laws of England*; emphases in the Oxford English Dictionary).

2. The use of §2703(d) orders for cell-tower records does not "diminish[] the degree of privacy that individuals reasonably expected prior to the" invention and widespread dissemination of mobile phones (Pet. Br. 10). *See Kyllo*, 533 U.S. at 34. The cell-tower records Petitioner sought to exclude show that a particular phone used certain towers belonging to the phone company "at call origination and at call termination for incoming and outgoing calls." *United States v. Carpenter*, 819 F.3d 880, 884, 886 (6th Cir. 2016). Before cell phones were invented, Petitioner could not have made or received the calls in question without revealing location-related information to a third-party service provider. Instead, Petitioner would have had to use stationary landline telephones tied to fixed locations; and calls using such phones would have generated third-party records revealing much more precise location-related information than the general vicinity information circumstantially discernible from cell-tower records. *See Smith*, 442 U.S. at 737; *Graham*, 846 F. Supp. 2d, at 399.

In other words, Petitioner did not lose anything in the way of preexisting Fourth Amendment rights when he chose to use a cell phone to make and get calls before, during, and after he committed the robberies of

which he was convicted—and while he was still close to the scene of each crime. That is because Petitioner could not have lost what he never had; and he never had a Fourth Amendment right to make or get a call without revealing to a third-party service provider location-related information incidental to the transmission of that communication. *See Smith*, 442 U.S. at 744–45.

C. This Court's third-party doctrine need not be construed to defeat more substantial expectations of privacy not at issue in this case.

There is nothing troubling about applying the third-party doctrine to uphold the congressionally regulated and judicially supervised investigative tool at issue here. Under the statutory procedure the government invoked in this case, a phone company may not be required to disclose any of its own cell-tower data to the government unless and until all three branches of the government acquiesce in the disclosure. *See* §2703(d). Congress must have authorized the issuance of a requested court order; a law-enforcement officer serving in the executive branch must determine that it is proper to invoke that statutory authority in the particular circumstances at hand; and a neutral and detached magistrate serving in the judicial branch must find that the government has adduced "specific and articulable facts" establishing "reasonable grounds to believe" that the requested third-party records are "relevant and material to an ongoing *criminal* investigation," *i.e.*, to an inquiry that implicates particularly compelling interests in exonerating the innocent, apprehending the guilty, and protecting the public. *See* 18

U.S.C. §2703(d) (emphasis added). Under established Fourth Amendment principles, that statutory procedure does not *lower* the bar from a warrant to a §2703(d) order; it *raises* the bar from an ordinary subpoena to one that incorporates a broad range of additional privacy protections. *Davis*, 785 F.3d at 505–06.

Future cases, which could involve more sensitive data obtained without the safeguards of the SCA, may well raise distinct concerns. Accordingly, this Court should exercise caution in articulating the contours of the third-party doctrine. As the federal Courts of Appeals have recognized, that doctrine need not be construed to defeat more substantial privacy concerns that are not implicated by compulsory process for the disclosure of cell-tower records under the SCA. *See, e.g.*, *Davis*, 785 F.3d at 505 (distinguishing cases involving the use a GPS device, a physical trespass, or real-time or prospective location tracking); *United States v. Warshak*, 631 F.3d 266, 282–86 (6th Cir. 2010) (requiring warrant before obtaining contents of email communications from an email service provider).

The "reality" of the investigative tool at issue here "hardly suggests abuse." *See United States v. Knotts*, 460 U.S. 276, 283 (1983). Indeed, the whole point of the SCA is to *prevent*—not to *permit*—"unfettered" acquisition of potentially sensitive third-party information. That is why, to take just one example, the SCA generally prohibits private phone companies from *voluntarily* sharing their own data with "a governmental entity." *See* 18 U.S.C. §2702(c)(4), (6); *see also, e.g.*, Vt. Stat. tit. 12, §8102(f). "As that prohibition underscores, a telephone company (like MetroPCS) would,

absent privacy-protecting laws (like the SCA), be free to disclose its historical cell tower location records to governmental and non-governmental entities alike—without any judicial supervision," "without having to satisfy the statutory standard in §2703(d)," and without even implicating the Fourth Amendment. *Davis*, 785 F.3d at 506.

If and when Congress and the state legislatures seek to authorize, and private companies make possible, "dragnet type law enforcement practices," "there will be time enough then to determine whether different constitutional principles may be applicable." *Knotts*, 460 U.S. at 284. In the meantime, this Court's Fourth Amendment jurisprudence should be adapted to the realities of the world that we live in, not based on hypothetical scenarios that have nothing to do with facts of this case or the eminently reasonable investigative tool Petitioner asks this Court to strike down. *See id.*

II. THE CHALLENGED SCA ORDERS WERE CONSTITUTIONALLY REASONABLE.

A. The warrant procedure should not be mechanically applied to congressionally-authorized "searches" arising out of the issuance of compulsory process for third-party cell-tower records.

The Fourth Amendment bars *unreasonable* searches, not *warrantless* searches. *Kentucky v. King*, 131 S. Ct. 1849, 1858 (2011). Any arguable "search" of Petitioner arising out of a phone company's disclosure to the government of its own routing-related records

was constitutionally reasonable. At least three considerations support that conclusion.

First, the SCA goes "above and beyond" traditional constitutional prerequisites governing the issuance of compulsory process. *Davis*, 785 F.3d at 506 (discussing "privacy-protection provisions" of the SCA). "[T]he Fourth Amendment, *if applicable to subpoenas for the production of business records and papers, at the most* guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described,' if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant." *Miller*, 425 U.S. at 445–46 (emphasis added; quotation marks and brackets omitted).

It is not a problem that the SCA omits some of the protections ordinarily tied to the warrant procedure, such as the probable-cause standard and the requirement that facts be attested under oath. As applied to compulsory process, "[t]he requirement of 'probable cause, supported by oath or affirmation' literally applicable in the case of a warrant is satisfied, in that of an order for production, by the court's determination that the investigation is authorized by Congress, is for a purpose Congress can order, and the documents sought are relevant to the inquiry." *Walling*, 327 U.S. at 209. Petitioner's complaints concerning the SCA's departures from the warrant procedure ring particularly hollow in light of the warrant-like protection afforded by the statute. After all, "[t]he primary reason for the warrant requirement is to interpose a 'neutral and detached magistrate' between the citizen

and the 'officer engaged in the often competitive enterprise of ferreting out crime,'" *United States v. Karo*, 468 U.S. 705, 717 (1984), and the SCA does just that.

In short, the challenged court orders comply with applicable Fourth Amendment requirements. Hence, those orders are constitutionally reasonable, even if Petitioner has "the requisite Fourth Amendment interest to challenge the validity" of those orders. *Miller*, 425 U.S. at 446; *see also Walling*, 327 U.S. at 208.

Second, a traditional Fourth Amendment analysis independently supports the reasonableness of the challenged court orders. *See Wyoming v. Houghton*, 526 U.S. 295, 300 (1999). Petitioner "had at most a diminished expectation of privacy in business records made, kept, and owned by [a third-party service provider]; the production of those records did not entail a serious invasion of any such privacy interest, particularly in light of the privacy-protecting provisions of the SCA; [and] the disclosure of such records pursuant to a court order authorized by Congress served substantial governmental interests." *Davis*, 785 F.3d at 518.

Third, there is a "strong presumption of constitutionality due to an Act of Congress, especially when [a constitutional challenge] turns on what is 'reasonable'" within the meaning of the Fourth Amendment. *United States v. Watson*, 423 U.S. 411, 416 (1976). That "strong presumption" should weigh at least as heavily as the general default rule against warrantless searches. Indeed, deference to Congress is particularly appropriate when, as here, any arguable "search" is based on the amorphous "*Katz* standard," which asks

whether an "asserted expectation of privacy is one that *society* is prepared to recognize as reasonable.'" *Carpenter*, 819 F.3d at 889–90 (emphasis added; quotation marks omitted). In that context, "one might say that society itself—in the form of its elected representatives in Congress—has already struck a balance that it thinks reasonable." *Id.* at 890.

Petitioner is wrong to suggest that this case does not involve a congressionally-authorized production. The cell-tower records Petitioner sought to suppress were produced pursuant to a court order issued under 18 U.S.C. §2703(d). Pet. App. 36a. And Petitioner has not asked this Court to review the district court's ruling that the challenged court orders were authorized by statute. *See* Pet i; Pet. App. 39a-40a. Hence, the issue in this case is whether the SCA is unconstitutional insofar as it authorized the government to obtain the historical cell-tower records in question. *See* Pet. App. 36a. That issue implicates the "gravest and most delicate duty" this Court is called on to perform, *see Nw. Austin Mun. Utility Dist. No. One v. Holder*, 557 U.S. 193, 204 (2009) (quotation marks omitted), and calls for the full measure of deference to which congressional enactments are entitled.

B. As real-world examples make clear, Section 2703(d) orders for cell-tower records serve compelling governmental interests, at little or no cost to individual privacy.

"[L]ike other forms of compulsory process not subject to the warrant procedure," §2703(d) orders for cell-tower records are "particularly valuable during the early stages of an investigation," when they "help to

build probable cause against the guilty, deflect suspicion from the innocent, aid in the search for truth, and judiciously allocate scarce investigative resources." *Davis*, 785 F.3d at 518. Real-world examples help to show why that is so, and how such orders are used during the course of day-to-day law-enforcement investigations.

1. In 2011, law-enforcement authorities investigated a series of seven armored-car robberies in Atlanta, Georgia. During one of the robberies, one security guard was murdered and another suffered serious injuries resulting from multiple gunshot wounds. After identifying one of the possible suspects, the FBI obtained call-detail records reciting the phone numbers of people with whom the suspect had been communicating within an hour of each robbery. Investigators lacked probable cause to believe that those other people had committed a crime; but they reasonably suspected that the subject may have been communicating with confederates just before and after the robberies were committed. Accordingly, they obtained §2703(d) orders for approximately 20 people with whom the subject had been in contact during the times in question. Based on those records, the FBI preliminarily excluded 15 potential suspects and identified five additional suspects who were near the robberies and warranted additional investigation. The five additional suspects, along with the initial suspect, all pleaded guilty. (Source: FBI/CAST. N.D. Ga. Case No. 1:11-CR-255.)

2. In 2014, the so-called "Bulls Bandit" robbed two banks in California over a two-month period. Both times, the robber obtained cash from bank tellers after

threatening to detonate a bomb. The robber bore at least some resemblance to a parolee already known to law-enforcement authorities, but the FBI was not able to positively identify that parolee as the robber. Historical cell-tower records obtained under §2703(d) showed that the parolee's phone had communicated with towers near both of the victim banks around the times of the robberies. Based on that information as well as the physical resemblance, the FBI developed probable cause supporting a search warrant, which turned up evidence of the robberies. (Source: U.S. Attorney's Office for the Central District of California. *United States v. Jeremiah Edmond Colino*, Case No. 14-CR-359-PA.)

3. The Phoenix Serial Street Shooter case involved a series of nine shootings, linked together by forensic ballistics evidence, in which seven people were killed. During the investigation, law-enforcement authorities received multiple tips from various members of the public who chose not to identify themselves, presumably out of concern for their own safety. Agents also developed certain investigative leads based on purely circumstantial evidence, such as vehicle descriptions that matched the suspected vehicles, documents showing ownership of the suspected make and model of handguns used, review of social media postings, and previously filed police reports. Due to the anonymous nature of tips received from the general public, and the circumstantial nature of other evidence, agents likely lacked probable cause to believe that any particular suspect committed the shootings.

Cell-tower records obtained under §2703(d) were used to exclude at least two potential suspects. Another suspect could not be included or excluded using those

records; but law-enforcement officers focused other investigative resources on that suspect, which yielded additional physical and circumstantial evidence establishing probable cause to support an arrest. Subsequent investigation linked three additional shootings, resulting in two additional homicides, to the alleged shooter. (Source: FBI/CAST. Maricopa County Superior Court, *Arizona vs. Aaron Juan Saucedo*, Nos. CR2017002335 and CR2017118158.)

4. In March 2011, a warehouse in Wethersfield, Connecticut, was burglarized, and nearly $500,000 worth of cigarettes were stolen. The thief wore a mask, and he also disabled all but one of the surveillance cameras surrounding the warehouse. Twice during the burglary, he was caught on video while holding a cell phone to his ear. The two apparent calls were about an hour apart. With no other leads to go on, law-enforcement agents obtained cell-tower records from the major cell service providers in the area for those two narrow time frames. One number bearing an out-of-state area code showed up with outgoing calls around both time stamps matching the video footage; but it was a burner phone with no identifiable account holder. *See United States v. Oreckinto*, 2017 WL 131563, at *2 (D. Conn. Jan. 13, 2017). Agents then obtained additional call-detail records for that number and began focusing on frequently dialed numbers from the cell phone in question. One frequently dialed number was a family member of a man named Andrew Oreckinto. Agents used that information to find Oreckinto's spouse's Facebook page, which showed a photograph of Oreckinto wearing the same sweatshirt worn by the thief on the warehouse surveillance video. *See United States v. Oreckinto*, 234 F. Supp. 3d 360, 362–64 (D. Conn. 2017)

(denying Oreckinto's motion to exclude images of the sweatshirt).

Using cell-tower records, investigators also linked Oreckinto to three similar burglaries in Connecticut and Pennsylvania in 2009 and 2010. The same burner cell phone number was in the area of two of the burglaries at the time they were committed. A federal jury found Oreckinto guilty of theft of goods from an interstate shipment, in violation of 18 U.S.C. §659, and he also confessed to a 2008 copper theft in New Jersey. *See United States v. Oreckinto*, 2017 WL 1371255 (D. Conn. Apr. 14, 2017). (Source: U.S. Attorney's Office, District of Connecticut.)

Those examples help to illustrate several important points:

First, like other forms of compulsory process not subject to the warrant procedure, historical cell-tower records are an indispensable building block of probable cause. If law-enforcement officers must have probable cause to get such records in the first place, many crimes will never be solved. *See United States v. R. Enters.*, 498 U.S. 292, 297 (1991); *McMann v. Sec. & Exch. Comm'n*, 87 F.2d 377, 379 (2d Cir. 1937) (Hand, J.). And there will be many other cases in which probable cause is developed but comes too late—too late to prevent additional crimes against victims, too late to catch a suspect who has fled, or too late because of the intervening loss or deterioration of other relevant evidence.

Second, §2703(d) orders for cell-tower records frequently help to exonerate the innocent. *See Davis*,

785 F.3d at 518. In some cases, such records are sufficient to exclude potential suspects, and thus spare innocent parties from the substantial burdens of being subjected to a protracted criminal investigation. In others, they at least "deflect suspicion from the innocent," allowing agents to "judiciously allocate scarce investigative resources" by focusing on suspects more likely to be guilty. *See id.*

Third, §2703(d) orders, like other forms of compulsory process, complement rather than displace the warrant procedure. Combined with other evidence, law-enforcement officers routinely use records obtained via compulsory process to obtain probable-cause warrants authorizing more substantial invasions of individual privacy—like the physically disruptive search of a home, a wiretap intercepting the contents of a communication, or a tracking warrant allowing law-enforcement officers to determine the precise location of a telephone (and not just the general vicinity information circumstantially discernible from cell-tower records).

On the other hand, there is no evidence that SCA orders for cell-tower records have ever been abused to the detriment of legitimate privacy interests. In theory, it is possible that rogue law-enforcement officers could obtain such records for legitimate reasons, and then seek to mine them for personal information unrelated to an ongoing criminal investigation. But that same risk is present even if such records are disclosed—as Petitioner concedes is permissible—pursuant to a warrant based on probable cause. In addition, Petitioner does not point to any real-world example in which law-

enforcement authorities used cell-tower records to obtain sensitive information that was not "relevant and material to an ongoing criminal investigation," §2703(d). Nor does he point to any example in which such information was improperly shared in contravention of the statutory bar against improper disclosures. *See* 18 U.S.C. §2707(g). If any such abuse takes place, the SCA "provides remedies and penalties for violations of the Act's privacy-protecting provisions, including money damages and the mandatory commencement of disciplinary proceedings against offending federal officers." *Davis*, 785 F.3d at 506 (citing 18 U.S.C. §§ 2707(a), (c), (d), 2712(a), (c)).

C. Congress and the state legislatures should be free to craft reasonable legislative solutions to the difficult problems arising out of compulsory disclosure of third-party records.

As Petitioner sees it, "this Court should provide a 'simple' answer to the question presented: 'get a warrant.'" Pet. Br. 57–58 (quoting *Riley v. California*, 134 S. Ct. 2473, 2495 (2014)). No matter how this case comes out, the Court should decline Petitioner's invitation to reflexively and mechanically apply the warrant procedure to congressionally authorized searches deemed to arise out of the issuance of compulsory process for third-party business records.

As Congress and the state legislatures have recognized, judicial process for the production of third-party evidence implicates two competing interests, both of which are important. On the one hand, there is a societal interest in protecting the confidentiality of

customer-related information that is exposed to and captured by third-party service providers during the ordinary course of business. *See In re Application for Historical Cell Site Data*, 724 F.3d at 615. On the other hand, there is also a competing societal interest in allowing the government to use ordinary truth-seeking tools to compel the production of non-privileged evidence that is "relevant and material to an ongoing criminal investigation," §2703(d). *See United States v. Nixon*, 418 U.S. 683, 707–09 (1974). Such evidence, after all, is needed to exonerate the innocent and apprehend the guilty; and to do so sooner rather than later, before an innocent person is subjected to a protracted criminal investigation or wrongful incarceration, and before additional crimes are committed against innocent victims, who also—and no less than criminal suspects—have dignity and privacy rights that are deserving of protection. *See* Pet. App. 40a (noting that application recited evidence from a cooperating defendant that the suspects "planned to do additional robberies" and represented that "the cell site records are needed to assist in identifying and locating other persons involved in the robberies").

How should those competing societal interests be balanced? There is no one answer, much less a "'simple' answer," Pet. Br. 58, to that question. The better answer is: *It depends*—on the sensitivity of the information in question, the strength of the relevant societal expectation of privacy, how such evidence is obtained, how much such evidence helps to promote the ends of justice, whether statutory privacy protections accommodate legitimate confidentiality and dignity interests, and a myriad of other factors. All of those factors may change over time, and reasonable people

can disagree about how they should be balanced. *See United States v. Jones*, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring).

The approach Congress took in the SCA—breaking up the pertinent investigative power, allocating it among the three branches of government, and requiring unanimous interbranch cooperation *before* the government may compel a third party to produce any potentially sensitive evidence in its possession—embodies a particularly enlightened and elegant solution. This Court should defer to that eminently reasonable legislative scheme—not because the underlying question of public policy is easy, but because it is hard.

Petitioner's contrary approach would impose a rigid, permanent, one-size-fits-all solution on every state in the country. Such an approach is both unnecessary and unwise.

Congress and the state legislatures are fully capable of protecting sensitive location information. A number of states have enacted statutes specifically regulating the acquisition of location-related information. *E.g.*, Colo. Rev. Stat. §16-3-303.5(1)(d); Minn. Stat. §626A.42(1)(e); N.H. Rev. Stat. Ann. §644-A:61.V. Legislation addressing location data been increasingly common in recent years. *E.g.*, Conn. Stat. §54-47aa(a)(6), (b) (amendment effective October 1, 2017); 2014 Md. Laws Ch. 191 (enacting Md. Code Crim. P. §1-203.1); Minn. Stat. §626A.42 (2014) (new statute governing "Electronic Device Location Information"); N.H. Rev. Stat. Ann. §644-A (2015) (same).

States have adopted a variety of standards for obtaining location-related information. Those standards build on the protections of the SCA, affording greater protections that may stop short of requiring a full-blown warrant. For example, Connecticut law authorizes a judge to compel disclosure of certain "geolocation data" "if the judge makes a finding of probable cause to believe that a crime has been or is being committed and the . . . geolocation data . . . is relevant and material to an ongoing criminal investigation." Conn. Stat. §54-47aa(a)(5), (b) (amendment effective October 1, 2017). That law would seem to provide greater protection than §2703(d) inasmuch as it requires probable cause to believe that *a crime has been committed*. Like §2703(d), however, Connecticut's law does not appear to require probable cause to believe that *the owner or user of the phone has committed a crime* or that incriminating (as opposed to "relevant and material") evidence *will be found in the requested phone records*. *See id.* As Connecticut's solution suggests, reasonable people may disagree about *what* probable cause should look like as applied to the issuance of compulsory process, and not just *whether* probable cause should be required.

Other states have also built on but departed from the standard Congress enacted in §2703(d). Virginia, for example, authorizes a court to order a provider of an electronic communication service to disclose non-content records, excluding real-time location data, "if the investigative or law-enforcement officer shows that there is reason to believe the records or other information sought are relevant and material to an ongoing criminal investigation, *or* the investigation

of any missing child as defined in §52-32, missing senior adult as defined in §52-34.4, or an incapacitated person as defined in §64.2-2000 who meets the definition of a missing senior adult except for the age requirement." Va. Code Ann. §19.2-70.3(B) (emphasis added). As the text after the italicized "or" makes clear, Virginia lawmakers have found that weighty societal interests other than exonerating the innocent and apprehending the guilty—e.g., finding a "missing child" or other vulnerable member of society—may support compulsory disclosure of third-party records.

Legislatures have distinguished between different kinds of "location information," concluding that some deserve more protection than others. For example, it is not uncommon for states to provide greater protections when the government seeks to track an individual by obtaining real-time location information (as opposed to the historical records at issue here). Illinois law provides that "a law enforcement agency shall not obtain current or future location information . . . without first obtaining a court order . . . based on probable cause to believe that the person whose location information is sought has committed, is committing, or is about to commit a crime," or in certain other statutorily specified circumstances. 725 Ill. Comp. Stat. 168/10; *see* Va. Code Ann. § 19.2-70.3(E) (providing that "an investigative or law-enforcement officer may obtain real-time location data without a warrant" only in certain limited circumstances).

As some state laws reflect, the standard by which law-enforcement authorities may obtain third-party records may turn in part on the legislature's assessment of how important it is to investigate a

particular kind of crime. Utah law, for example, generally provides that "a government entity may not obtain" certain "stored data, or transmitted data of an electronic device without a search warrant issued by a court upon probable cause." Utah Code Ann. §77-23c-102(1)(a). But the statute contains an exception authorizing a "prosecutor" to "obtain a judicial order" for certain non-location stored data "[w]hen a law enforcement agency is investigating a sexual offense against a minor, an offense of stalking . . . , or an offense of child kidnapping . . . , and has reasonable suspicion" that a certain kind of communication service "has been used in the commission of a criminal offense." *See id.* §77-22-2.5(2); §77-23c-102(1)(a), (2). If those criteria are satisfied, the law provides that a "law enforcement agent shall" follow procedures akin to—and expressly referencing—"18 U.S.C. § 2703." *Id.* §77-22-2.5(2)(a), (b), (c).

Like Congress, the state legislatures have enacted a broad range of measures to ensure that third-party records are used and handled properly. For example, some states regulate what law-enforcement officers may do with location-related information obtained from a third-party service provider, *e.g.*, Cal. Penal Code. §1546.1(d)(2); La. Rev. Stat. §844.9B.(4)–(5); Utah Code Ann. §77-23c-102(1)(b); require or provide for records to be destroyed within a certain period of time, subject to certain qualifications, *e.g.*, Cal. Penal Code §§1546.1(e)(2), (g); Utah Code Ann. §77-23c-102(1)(d); Vt. Stat. Ann. tit. 13, §8102(g); and mandate that notice be provided to ensure that affected parties are informed in a manner that does not unduly compromise an ongoing investigation, *e.g.*, Conn. Gen. Stat. §54-47aa(f); Md. Code Ann. Crim. §1-203.1(d); Me. Rev.

Stat. tit. 16 §649; R.I. Gen. Laws §12-32-3; Vt. Stat. Ann. tit. 13, §8103.

In short, Congress and the state legislatures are up to the task of protecting legitimate confidentiality interests implicated by compulsory process for third-party business records revealing location-related information. The "simple answer" Petitioner favors—importing, for the very first time, the warrant requirement into the well-established legal regime governing the issuance of compulsory process for third-party records—threatens to cast a cloud of doubt over any number of valuable federal and state laws, to upend centuries of practice, and to preempt ongoing efforts to craft legislative solutions that strike a sensible balance between critical law-enforcement needs and competing confidentiality interests.

D. Reasonable considerations support the application for longer-term records in cases like this one.

The four-month time span of the records at issue here does not make the challenged court orders unreasonable.

Petitioner has not challenged the lower court's ruling that the SCA authorized the issuance of a court order compelling the production of the records at issue here. *See* Pet. i; Pet. App. 39a-40a. Thus, it is undisputed that a federal magistrate judge properly found that the government had adduced "specific and articulable facts" establishing "reasonable grounds to believe" that the requested records were "relevant and material to an ongoing criminal investigation," §2703(d).

In cases like this one, there are good reasons for seeking "longer-term" records of the kind at issue here.

First, longer-term records help investigators to ascertain the identity of the phone user. As noted above, modern criminals frequently obtain disposable burner phones registered under a fictitious alias. And, even when they do not, a mobile phone may regularly be used by someone not listed as the official subscriber. Longer-term cell-tower data help to test allegations or hypotheses that a particular phone belonged to a particular person, by showing whether that phone—even when it was not being used to perpetrate a crime under investigation—was in an area to which that person could be tied by other evidence.

Second, longer-term records help to make sense of the general vicinity information circumstantially discernible from cell-tower records. In rural areas, "a tower's coverage might reach as far as 20 miles." *Carpenter*, 819 F.3d at 885. In urban areas, "each cell site covers 'typically anywhere from a half-mile to two miles.'" *Id.* In either case, cell-tower records show only that a phone was "in the general area" of the place where a crime took place. Pet. App. 45a. Accordingly, short-term cell-tower records have the potential to be misleading. After all, and as defense attorneys frequently argue to juries, a suspect may have had an entirely innocent reason for being in the area in question; for example, he may have lived or worked in that area, or may have been visiting friends or family members.

Longer-term records help to assess those possibilities. Suppose, for example, that a phone was in the

vicinity of a crime scene only once over a two-month period—right around the time when the crime was committed. Such evidence would allow investigators and prosecutors to rule out, and would help juries to assess, the possibility that a suspect just happened to live or work in that area. Similarly, suppose that a phone tied to a suspect was near the scene of many different crimes committed at different times in different locations served by different towers. Such evidence would tend to refute allegations that a suspect just happened to be visiting the neighborhood where any particular crime took place at the time in question. Finally, suppose that a suspect was frequently in the vicinity of the spot where an isolated crime occurred. Such evidence might well support a jury's decision to discount short-term cell-tower data otherwise tending to corroborate the inculpatory testimony of an accomplice.

In short, "longer-term" cell-tower records help investigators and prosecutors (at the front end) and juries and judges (at the back end) to make sense of cell-tower records of the kind at issue here; and that is the case precisely because "shorter-term" cell-tower records, standing alone, cannot be used to conclusively determine the identity or precise location of a phone user.

Petitioner is not in a good position to argue otherwise. Like many modern-day criminals, Petitioner used a phone that was registered under a different name. Pet. App. 76a. And, like many criminal defendants seeking to suppress inculpatory cell-tower records, Petitioner did not admit that the phone in question was his. *See supra* at 8. Although confederates

implicated Petitioner in the charged offenses and testified that the phone in question was his, Petitioner argued that such testimony was unreliable because the robbers were facing "enormous pressure" to lie. *Filings of Defendant, United States v. Carpenter*, No. 12-cr-20218 (E.D. Mich.), ECF No. 333, at 62. And, as is often the case when the prosecution introduces cell-tower evidence, Petitioner's argument to the jury was that the government had erred by analyzing *too little*—and *not too much*—cell-tower data. In closing argument, for example, counsel for Petitioner faulted the government's expert witness because he "didn't put in . . . other records of cell phone calls" on the days in question. *Id.* at 78–79. The agent, defense counsel charged, "wasn't interested in" whether the records, taken as a whole, supported the prosecution's theory, so he included cell-tower data when it supported that theory, but "left it out" when pertinent evidence "didn't fit his theory." *Id.* at 79.

The "longer-term" cell-tower records Petitioner sought to suppress were assuredly "relevant and material" to that defense. Indeed, the government was duty-bound to carefully consider such evidence on its own, before it relied on "shorter-term" cell-tower records as a large part of its case for depriving Petitioner of his liberty.

III. Section 2703(d) Is Not Unconstitutional in All Its Applications to Cell-Tower Records.

Assuming *arguendo* that Section 2703(d) is unconstitutional as applied to "the acquisition of longer-term cell site location information," Pet. Br. 14, this

Court should leave the statute intact as applied to the acquisition of shorter-term cell-tower location data. Petitioner concedes that there is at least "some period of time" over which cell-tower records may be obtained without implicating the Fourth Amendment, *id.* at 30 (quotation marks omitted). And it is a "fundamental principle of judicial restraint" that "courts should neither anticipate a question of constitutional law in advance of the necessity of deciding it nor formulate a rule of constitutional law broader than is required by the precise facts to which it is to be applied." *Wash. State Grange v. Wash. State Republican Party*, 552 U.S. 442, 450 (2008) (quotation marks omitted).

On the merits, there is no viable basis for holding that third-party cell-tower data is always within the phone user's reasonable expectation of privacy—no matter whether the information in question pertains to a single phone call spanning a few seconds or thousands of phone calls spanning a few years, no matter whether the subscriber makes a call in plain view in a public place or from the privacy of his own home, and no matter how explicit the warning incorporated into the customer's service contract. Indeed, such a holding cannot be reconciled with established Fourth Amendment principles.

For example, it is settled law that the police may monitor the whereabouts of suspects traveling in public areas over relatively short periods of time with the aid of electronic devices *surreptitiously* installed in items those suspects obtained from third parties—even if such real-time surveillance is conducted without any judicial supervision or legislative authorization. *See Karo*, 468 U.S. at 707, 712–14); *Knotts*, 460 U.S. at

281–85. In *Jones*, all nine members of this Court stood by that prior precedent. *See* 464 U.S. at 410 ("Karo accepted the container as it came to him, beeper and all, and was therefore not entitled to object to the beeper's presence, even though it was used to monitor the container's location" without his knowledge); *id.* at 430 (Alito, J., concurring in the judgment) (citing *Knotts*, 460 U.S. at 281–82, for the proposition that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable"). *A fortiori*, investigative agents should be able to obtain the same kind of location information from cell-phone-related technologies of which phone users are expressly and unambiguously warned, particularly when that information is obtained from a third party pursuant to a court order authorized by Congress in a privacy-protecting statute.

CONCLUSION

The judgment of the Court of Appeals should be affirmed.

Respectfully submitted,

PAMELA JO BONDI
Attorney General of Florida

AMIT AGARWAL
Solicitor General
**Counsel of Record*
DENISE M. HARLE
JORDAN E. PRATT
Deputy Solicitors General

Office of the Attorney General
PL-01, The Capitol
Tallahassee, Florida 32399
Amit.Agarwal@myfloridalegal.com
(850) 414-3300

STEVE MARSHALL
Attorney General of Alabama

MARK BRNOVICH
Attorney General of Arizona

CYNTHIA H. COFFMAN
Attorney General of Colorado

LAWRENCE G. WASDEN
Attorney General of Idaho

CURTIS T. HILL, JR.
Attorney General of Indiana

DEREK SCHMIDT
Attorney General of Kansas

ANDY BESHEAR
Attorney General of Kentucky

BRIAN E. FROSH
Attorney General of Maryland

BILL SCHUETTE
Attorney General of Michigan

TIMOTHY C. FOX
Attorney General of Montana

DOUG PETERSON
Attorney General of Nebraska

GORDON J. MACDONALD
Attorney General of New Hampshire

HECTOR H. BALDERAS
Attorney General of New Mexico

MIKE HUNTER
Attorney General of Oklahoma

JOSH SHAPIRO
Attorney General of Pennsylvania

ALAN WILSON
Attorney General of South Carolina

HERBERT H. SLATERY III
Attorney General and Reporter
of Tennessee

PETER K. MICHAEL
Attorney General of Wyoming

October 2, 2017

RECORD AND BRIEFS

FILED
AUG 14 2017
OFFICE OF THE CLERK
SUPREME COURT, U.S.

No. 16-402

In The
Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ Of *Certiorari* To The United States Court Of Appeals For The Sixth Circuit

---

BRIEF OF THE CENTER FOR COMPETITIVE POLITICS, CENTER FOR MEDIA JUSTICE, COLOR OF CHANGE, AMERICANS FOR PROSPERITY FOUNDATION, AND TEA PARTY PATRIOTS IN SUPPORT OF PETITIONER

ALLEN DICKERSON
Counsel of Record
ZAC MORGAN
CENTER FOR COMPETITIVE POLITICS
124 S. West St., Ste. 201
Alexandria, VA 22314
adickerson@campaignfreedom.org
(703) 894-6800
Counsel for Amici Curiae

August 14, 2017

LEGAL PRINTERS LLC, Washington DC • 202-747-2400 • legalprinters.com

TABLE OF CONTENTS

Table of Authorities ii
Interest of *Amici Curiae* 1
Summary of the Argument 3
Argument 5

I. Cell site location data allows the government to pinpoint an individual's associations with extraordinary precision 5

II. In addition to the Fourth Amendment concerns raised in the Petition, the government's ability to obtain archived, granular location data for the bulk of the American population poses a grave risk to First Amendment associational liberties .. 7

a. Freedom of association is protected by the First Amendment 8

b. The government's ability to review citizens' every movement is likely to chill this constitutionally protected right 11

III. Requiring the government to obtain a warrant before viewing, analyzing, or acting upon geolocational data will safeguard freedom of association 13

Conclusion 14

TABLE OF AUTHORITIES

Cases

Am. Civil Liberties Union v. Clapper,
785 F.3d 787 (2d Cir. 2015) 9

Baird v. State Bar of Ariz.,
401 U.S. 1 (1971) 9

Bates v. City of Little Rock,
361 U.S. 516 (1960) 4, 8, 9

Bond v. Floyd,
385 U.S. 116 (1966) 10

Brown v. Socialist Workers '74 Campaign Comm.,
459 U.S. 87 (1982) 10

Buckley v. Valeo,
424 U.S. 1 (1976) 7, 8, 14, 15

Calif. Bankers Ass'n v. Shultz,
416 U.S. 21 (1974) 11

Fed. Election Comm'n v. Wisc. Right to Life, Inc.,
551 U.S. 449 (2007) 10

Gibson v. Fla. Legis. Investigation Comm.,
372 U.S. 539 (1963) 8, 9

In re Primus,
436 U.S. 412 (1978) 10

Keyishian v. Bd. of Regents of the Univ. of the State of N.Y.,
385 U.S. 589 (1967) 10

Kusper v. Pontikes,
414 U.S. 51 (1973) 7, 8

Lady J. Lingerie v. City of Jacksonville,
176 F.3d 1358 (11th Cir. 1999) 10

Mills v. Ala.,
384 U.S. 214 (1966) 12

NAACP v. Ala.,
357 U.S. 449 (1958) ..... *passim*

NAACP v. Button,
371 U.S. 415 (1963) 4, 10

N.Y. Times Co. v. Sullivan,
376 U.S. 254 (1964) 12

Rankin v. McPherson,
483 U.S. 378 (1987) 10

Riley v. Calif.,
134 S. Ct. 2473 (2014) 5, 13

Shelton v. Tucker,
364 U.S. 479 (1960) 7

Trinity Lutheran Church of Columbia, Inc. v. Comer,
137 S. Ct. 2012 (2017) 10

United States v. Graham,
824 F.3d 421 (4th Cir. 2016) 6

United States v. Harriss,
347 U.S. 612 (1954) 9

United States v. Karo,
468 U.S. 705 (1984) 13

United States v. Jones,
565 U.S. 400 (2012) 5, 13

United States v. Rumely,
345 U.S. 41 (1953) 9

Other Authorities

Associated Press, "Mozilla CEO resignation raises free speech issues",
USA Today, Apr. 4, 2014..... 12

Edmund Burke,
Reflections on the Revolution in France
(J.G.A. Pocock, ed., Hackett Publishing Co. 1987)..... 7

INTEREST OF *AMICI CURIAE*[1]

The Center for Competitive Politics is a nonpartisan, nonprofit organization that works to protect and defend the First Amendment rights of speech, assembly, and petition. As part of that mission, the Center represents individuals and civil society organizations, *pro bono*, in cases raising First Amendment objections to burdensome regulation of core political activity.

The Center for Media Justice (CMJ) is a national racial justice network hub taking action for 21st century media and technology rights, access and representation. Founded in 2008, CMJ is home to the Media Action Grassroots Network (MAG-Net) – the largest racial justice network for media, technology and cultural change in the United States. CMJ's mission is to win communication rights and representation for under-represented communities, with dignity and power for all. CMJ mobilizes and supports media justice campaigns, and strengthens the power of racial justice movements to win media rights and representation through network organizing, collective action, and capacity building.

Color Of Change is the nation's largest online racial justice organization and represents over one million members. As a national online force, the organization moves decision-makers in corporations and government to create a more human and less hostile world for Black people in America. By

---

[1] No counsel for a party authored this brief in whole or part, nor did any person or entity, other than *amici* or its counsel, financially contribute to preparing or submitting this brief. Both parties have provided written consent to the filing of this brief.

United States v. Graham,
824 F.3d 421 (4th Cir. 2016) 6

United States v. Harriss,
347 U.S. 612 (1954) 9

United States v. Karo,
468 U.S. 705 (1984) 13

United States v. Jones,
565 U.S. 400 (2012) 5, 13

United States v. Rumely,
345 U.S. 41 (1953) 9

Other Authorities

Associated Press, "Mozilla CEO resignation raises free speech issues",
USA Today, Apr. 4, 2014..... 12

Edmund Burke,
Reflections on the Revolution in France
(J.G.A. Pocock, ed., Hackett Publishing Co. 1987)..... 7

INTEREST OF *AMICI CURIAE*[1]

The Center for Competitive Politics is a nonpartisan, nonprofit organization that works to protect and defend the First Amendment rights of speech, assembly, and petition. As part of that mission, the Center represents individuals and civil society organizations, *pro bono*, in cases raising First Amendment objections to burdensome regulation of core political activity.

The Center for Media Justice (CMJ) is a national racial justice network hub taking action for 21st century media and technology rights, access and representation. Founded in 2008, CMJ is home to the Media Action Grassroots Network (MAG-Net) – the largest racial justice network for media, technology and cultural change in the United States. CMJ's mission is to win communication rights and representation for under-represented communities, with dignity and power for all. CMJ mobilizes and supports media justice campaigns, and strengthens the power of racial justice movements to win media rights and representation through network organizing, collective action, and capacity building.

Color Of Change is the nation's largest online racial justice organization and represents over one million members. As a national online force, the organization moves decision-makers in corporations and government to create a more human and less hostile world for Black people in America. By

---

[1] No counsel for a party authored this brief in whole or part, nor did any person or entity, other than *amici* or its counsel, financially contribute to preparing or submitting this brief. Both parties have provided written consent to the filing of this brief.

designing strategies powerful enough to fight racism and injustice—in politics and culture, in the work place and the economy, in criminal justice and community life, and wherever they exist—it is changing both the written and unwritten rules of society. Color Of Change mobilizes its members to end practices and systems that unfairly hold Black people back, and champion solutions that move us all forward.

Americans for Prosperity Foundation ("AFPF" or "the Foundation") is a 501(c)(3) nonprofit dedicated to promoting limited government and free markets. Because of the controversy surrounding its views, the Foundation and its known associates have repeatedly been subjected to vile, credible threats and even violent attacks. In an attempt to decrease these chilling effects, the Foundation actively protects its donors' and associates' confidentiality despite frequent governmental and media efforts to unmask them. Consistent with its mission of limited government, AFPF seeks to ensure the sanctity of the Bill of Rights, including preserving Fourth Amendment protections against unlawful government searches and seizures as well as safeguarding associational and expressive freedoms under the First Amendment, especially in the face of governmental overreach.

Tea Party Patriots represents over 3 million supporters and donors and over 800 locally affiliated groups. Many of these supporters meet with their local groups in quarterly, monthly, or weekly meetings where they discuss the issues we face as a nation, debate the merits of various solutions, and organize to spur action on the solutions we support. The organization and many of its affiliates also use

rallies as a tactic for spurring action by government officials. The organization believes in a country that protects personal and economic freedoms. It believes the freedom to associate is vital for its continued effectiveness. The group and many of its local affiliates were targeted by the IRS for their political beliefs, which greatly harmed their ability to operate. It is concerned that some government officials would use cell site location information to intimidate supporters or potential supporters from attending these meetings and rallies.

Amici have an interest in this case because the government's unhindered ability to collect and use cell site location data threatens to chill the First Amendment right to freedom of association.

SUMMARY OF THE ARGUMENT

Wireless service providers track all Americans carrying cellular phones—that is, virtually all of us. That information can pinpoint a person's location with great precision, and private companies store this data for years. In the future, this capability will expand, and the resulting information will potentially be stored in perpetuity.

While this case concerns the location of a single individual, that is not the only way in which locational data may be used. In a world where tracking information is so precise that individual rooms can be differentiated, the locations of multiple people can be amalgamated, allowing the government to assemble an extraordinarily precise picture of citizens' memberships, meetings, and associations.

Consequently, the government's warrantless access to this information threatens Americans' First

Amendment right "to pursue their lawful private interests privately and to associate freely with others in so doing." *NAACP v. Ala.*, 357 U.S. 449, 466 (1958). After all, associational liberty needs "breathing space to survive," *NAACP v. Button*, 371 U.S. 415, 433 (1963), and must be "protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference." *Bates v. City of Little Rock*, 361 U.S. 516, 523 (1960).

The warrantless collection of geolocational data from third parties risks short-circuiting these precedents and undermining the right to private association. This information offers governments the ability to reverse-engineer not merely groups' membership lists, but to also identify people with sympathy for or a passing interest in an organization's aims. Left unchecked, this power will discourage Americans from engaging in public gatherings and private meetings of all types, chilling both social and political association and the collective speech it fosters.

In recent Terms, this Court has not permitted the government to obtain a person's location or contacts on demand. That trend should continue, not only in the interest of the Fourth Amendment, but also to protect the First Amendment right to free and private association.

ARGUMENT

I. Cell site location data allows the government to pinpoint an individual's associations with extraordinary precision.

Virtually all Americans go about their day carrying a tracker in their pocket or purse. *Riley v. Calif.*, 134 S. Ct. 2473, 2490 (2014) ("According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time..."). A cell phone's "[h]istoric location information...can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Riley*, 134 S. Ct. at 2490. Allowing the government to freely access this data poses significant First Amendment concerns that necessitate the protections of a warrant requirement.

As Justice Sotomayor recognized in the context of warrantless GPS tracking, location data "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). In fact, cell site location data will soon be even more precise than the information collected in *Jones*. It will be able to show which meeting room at a community center a person visited, or what establishment in a strip mall she patronized. Pet. 7 ("Location precision is also increasing as service providers deploy millions of 'small cells,' 'which cover a very specific area, such as one floor of a building,

the waiting room of an office, or a single home'") (quoting *United States v. Graham*, 824 F.3d 421, 448 (4th Cir. 2016) (*en banc*) (Wynn, J., dissenting in part and concurring in the judgment); Pet. 8 ("The prosecutor argued to the jury, for example, that Mr. Carpenter was 'right where the first robbery was at the exact time of the robbery, the exact sector'").

And while it would be difficult for the government to install GPS devices under practically all private motor vehicles in the United States, allowing unwarranted access to cell site location data gives the government the same reach, combined with the ability to search through years of past data. Electronic Frontier Found. *Amicus* Br. in Supp. of Cert. 5 (noting "estimated 378 million...mobile device accounts in the United States"); *id.* at 10 ("Cell providers store this date for up to five years and can also track CSLI [Cell Site Location Information] in near real-time") (brackets supplied). There is every reason to believe that the precision of cell site location data, as well as the length of time for which it can be stored, will only increase in years to come. *Id.* at 10-11 (describing recent "advances" increasing reliability and specificity of cell site location information).

Carte blanche governmental access to this information raises significant First Amendment concerns. Because this data can be amalgamated—as happened here, where records for a number of people were simultaneously collected—requests for cellular location data can provide an extraordinarily precise picture of citizens' memberships, meetings, and associations. Such access is dangerous: "[e]ffective advocacy of both public and private points of view, particularly controversial ones, is

undeniably enhanced by group association." *NAACP*, 357 U.S. at 460. The government's ability to call up a person's geolocation history at will unquestionably functions to chill those gatherings, a result that both violates the First Amendment and poses a substantial threat to a vibrant civil society.[2]

II. In addition to the Fourth Amendment concerns raised in the Petition, the government's ability to obtain archived, granular location data for the bulk of the American population poses a grave risk to First Amendment associational liberties.

The right of all Americans "to pursue their lawful private interests privately and to associate freely with others in so doing," *NAACP*, 357 U.S. at 466, is a "basic constitutional protection[]," *Kusper v. Pontikes*, 414 U.S. 51, 57 (1973), that "'lies at the foundation of a free society.'" *Buckley v. Valeo*, 424 U.S. 1, 25 (1976) (*per curiam*) (quoting *Shelton v. Tucker*, 364 U.S. 479, 486 (1960)). Consequently, this Court has long protected the right not only to associate, but to do so privately, free from government surveillance or interference.

---

[2] *See* Edmund Burke, *Reflections on the Revolution in France*, 41 (J.G.A. Pocock, ed., Hackett Publishing Co. 1987) ("...to love the little platoon we belong to in society, is the first principle (the germ as it were) of public affections. It is the first link in the series by which we proceed towards a love to our country, and to mankind").

a. Freedom of association is protected by the First Amendment.

This Court first explicitly enumerated the contours of this "basic constitutional protection" in a series of decisions in the 1950's and 1960's. Those cases stemmed from the efforts of segregationist Southern governments to obtain the membership lists of civil rights organizations through corporate registration laws (*NAACP v. Alabama*), legislative investigations (*Gibson v. Florida Legislative Investigation Committee*, 372 U.S. 539 (1963)), and the taxing power (*Bates v. City of Little Rock*, 361 U.S. 516 (1960)).

These precedents established that associational liberty cannot be abridged for naught, and that government action potentially infringing on free association will be "subject to the closest scrutiny." *NAACP*, 357 U.S. at 461. Governments must tread carefully when condoning or conducting activities that touch upon that protected freedom, even in contexts less dire than those faced by the NAACP. *E.g. Kusper*, 414 U.S. at 57 (holding, where a citizen was prevented from voting in a different party's primary less than 23 months after casting her last vote, that "unduly restrictive state election laws may so impinge upon freedom of association as to run afoul of the First and Fourteenth Amendments").[3]

---

[3] Indeed, this Court has relied upon *NAACP v. Alabama* to facially rewrite campaign finance disclosure laws, reasoning that overly expansive disclosure demands "can seriously infringe on privacy of association and belief guaranteed by the First Amendment" *Buckley v. Valeo*, 424 U.S. 1, 64 (1976) (*per curiam*).

Whenever a "State attempts to make inquiries about a person's beliefs or associations, its power is limited by the First Amendment." *Baird v. State Bar of Ariz.*, 401 U.S. 1, 6 (1971). Such "sweeping state inquiries into these protected areas...discourage citizens from exercising rights protected by the Constitution." *Baird*, 401 U.S. at 6. Even when the government claims that its activities are backed by interests of the highest order, associational liberty may nevertheless trump. *See Am. Civil Liberties Union v. Clapper*, 785 F.3d 787, 802 (2d Cir. 2015) (relying on *NAACP v. Alabama* to permit, in national security context, First Amendment claim against government metadata collection because of the Plaintiff's "members' interests in keeping their associations and contacts private").

Accordingly, freedom of association is "protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference." *City of Little Rock*, 361 U.S. at 523.[4] "The strong associational interest in maintaining the privacy of membership lists of groups engaged in the constitutionally protected free trade in ideas and beliefs" belongs to "all legitimate organizations." *Gibson*, 372 U.S. at 555-556, and "it is immaterial whether the beliefs sought to be advanced

---

[4] As the *NAACP* Court noted, "recognition of possible unconstitutional intimidation of the free exercise of the right to advocate underlay this Court's narrow construction of the authority of a congressional committee investigating lobbying and of an Act regulating lobbying, although *in neither case* was there an effort to suppress speech." 357 U.S. at 461 (emphasis supplied) (citing *United States v. Rumely*, 345 U.S. 41, 46-47 (1953) and *United States v. Harriss*, 347 U.S. 612, 625-626 (1954)).

by association pertain to political, economic, religious[,] or cultural matters." *NAACP*, 357 U.S. at 462.

The *NAACP* and *Buckley* cases protect not merely controversial political dissent, *e.g. Brown v. Socialist Workers '74 Campaign Comm.*, 459 U.S. 87 (1982), but also more prosaic groups. For instance, the Eleventh Circuit has ruled that a city violated the First Amendment when it sought to "require[] corporate applicants for adult business licenses to disclose the names of 'principal stockholders'" privately to a regulatory agency, and invalidated the ordinance when the agency was unable to demonstrate a sufficient need for that information. *Lady J. Lingerie v. City of Jacksonville*, 176 F.3d 1358, 1366 (11th Cir. 1999) (citation omitted).[5]

---

[5] That associational liberty is granted such a wide berth is unsurprising. This Court has repeatedly stated that "First Amendment freedoms need breathing space to survive." *Button*, 371 U.S. at 433; *Fed. Election Comm'n v. Wisc. Right to Life, Inc.*, 551 U.S. 449, 468-469 (2007) (Roberts, C.J., controlling op.) (quoting same); *In re Primus*, 436 U.S. 412, 432 (1978) (quoting same); *Gooding v. Wilson*, 405 U.S. 518, 522 (1972) (quoting same); *Keyishian v. Bd. of Regents of the Univ. of the State of N.Y.*, 385 U.S. 589, 604 (1967) (quoting same); *Rankin v. McPherson*, 483 U.S. 378, 387 (1987) ("'Just as erroneous statements must be protected to give freedom of expression the breathing space it needs to survive, so statements criticizing public policy and the implementation of it must be similarly protected'") (quoting *Bond v. Floyd*, 385 U.S. 116, 136 (1966)). This Court reaffirmed this principle just this Term in the free exercise context. *Trinity Lutheran Church of Columbia, Inc. v. Comer*, 137 S. Ct. 2012, 2024 (2017) ("The Missouri Department of Natural Resources has not subjected anyone to chains or torture on account of religion. And the result of the State's policy is nothing so dramatic as the denial of political office...").

b. The government's ability to review citizens' every movement is likely to chill this constitutionally protected right.

If a state government tried to obtain the membership list of the Council on American-Islamic Relations, the Becket Fund, the American Civil Liberties Union, Planned Parenthood, the Heritage Foundation, Black Lives Matter, or some other issue group, whether through foreign corporation statutes, the taxing power, or other means, it would be rebuffed by courts following established precedent. *See Calif. Bankers Ass'n v. Shultz*, 416 U.S. 21, 98 (1974) (Marshall, J., dissenting) ("The First Amendment gives organizations such as the ACLU the right to maintain in confidence the names of those who belong or contribute to the organization, absent a compelling governmental interest requiring disclosure"); *NAACP*, 357 U.S. at 462 ("Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs").

But permitting governments to obtain the geolocational data of individuals that attend political meetings and events provides an opportunity to short-circuit these cornerstone precedents and reverse-engineer not only the membership list of a targeted group, but also identify those with sympathy for or a passing interest in the organization. A single group meeting, for instance, can be documented and archived. *See* Electronic Frontier Found. *Amicus* Br. in Supp. of Cert. 10-11.

In the instant matter, the government obtained 127 days of location history, and such data is stored

by private companies for up to five years. Going forward, we must assume that as the capacity to collect and archive this data grows, it will soon be possible for geolocational data to be held more-or-less permanently.

In such circumstances, declining to engage in public gatherings and private meetings may well become a rational choice for a broad range of opinion holders, including those who may presently exist within the mainstream of political thought. Today's majority opinion, after all, can rapidly become tomorrow's minority view. Associated Press, "Mozilla CEO resignation raises free-speech issues", USA Today, Apr. 4, 2014 (recounting controversy surrounding the resignation of Brendan Eich as CEO of Mozilla after his political donations in support of a successful California constitutional amendment became public knowledge).[6]

Such outcomes are precisely what this Court has sought to prevent. Chilling effects from this invasive form of government oversight will do grave damage to the First Amendment, which was designed to safeguard our "profound national commitment to the principle that debate on public issues should be uninhibited..." *N.Y. Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964); *Mills v. Ala.*, 384 U.S. 214, 218 (1966) ("Whatever differences may exist about interpretations of the First Amendment, there is practically universal agreement that a major purpose of that Amendment was to protect the free discussion of governmental affairs").

---

[6] *Available at:* https://www.usatoday.com/story/news/nation/2014/04/04/mozilla-ceo-resignation-free-speech/7328759/.

III. Requiring the government to obtain a warrant before viewing, analyzing, or acting upon geolocational data will safeguard freedom of association.

In recent Terms, this Court has limited the government's ability to determine a person's location or contacts on demand. *United States v. Jones*, 565 U.S. 400 (2012) (installing GPS device on car constitutes a search under the Fourth Amendment); *Riley v. Calif.*, 134 S. Ct. 2473 (2014) (Fourth Amendment requires that police obtain a warrant before searching data, including geolocational data, stored on a smartphone); *United States v. Karo*, 468 U.S. 705, 714 (1984) (warrantless "monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment..."). Had these cases been decided differently, more than the Fourth Amendment would have been affected. These rules would have directly impacted the ability of all Americans to associate with whomever they choose, free of government interference or surveillance, in their efforts to "advance[]...political, economic, religious[,] or cultural matters." *NAACP*, 357 U.S at 466. In this case, as in those, procedural protections are vital.

NAACP v. Alabama, once again, is instructive. Because a judicial forum was available, the NAACP was able to challenge the State of Alabama's subpoena of its membership list. *See Buckley*, 424 U.S. at 25 ("[G]overnmental 'action which may have the effect of curtailing the freedom to associate'" must be "'subject to the closest scrutiny'") (quoting *NAACP*, 357 U.S. at 460-461). Had the State of Alabama been able to simply obtain that information from a third

party, this important judicial check would have been unavailable, and the "likelihood of a substantial restraint" upon NAACP members' "right to freedom of association" would have been far higher. 357 U.S. at 462. Only a robust judicial backstop prevented that outcome.

CONCLUSION

The rights protected by the First Amendment function as an interlocking mechanism that protects our polity as a whole. Here, requiring the government to obtain a warrant before obtaining geolocational data will do more than vindicate the Fourth Amendment rights already explained by the Petitioner. That limitation will also guard against the "significant encroachments on First Amendment rights of the sort that compelled disclosure" of private information "imposes." *Buckley*, 424 U.S. at 64.

Respectfully submitted,

ALLEN DICKERSON
Counsel of Record
ZAC MORGAN
CENTER FOR
COMPETITIVE POLITICS
124 S. West St., Ste. 201
Alexandria, VA 22314
adickerson
@campaignfreedom.org
(703) 894-6800

August 14, 2017

Counsel for Amici Curiae

RECORD AND BRIEFS

Supreme Court, U.S.
FILED
AUG 14 2017
OFFICE OF THE CLERK

No. 16-402

In the Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Sixth Circuit

BRIEF OF THE CENTER FOR DEMOCRACY AND TECHNOLOGY AS *AMICUS CURIAE* IN SUPPORT OF PETITIONER

ANDREW J. PINCUS
Counsel of Record
Mayer Brown LLP
1999 K Street, NW
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com

Counsel for Amicus Curiae

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES iii

INTEREST OF THE *AMICUS CURIAE* 1

INTRODUCTION AND SUMMARY OF ARGUMENT 1

ARGUMENT 6

THE FOURTH AMENDMENT'S WARRANT REQUIREMENT APPLIES TO THE CELL PHONE LOCATION DATA AT ISSUE HERE 6

A. Broad Categories Of Highly Sensitive Personal Information About Virtually Every American Are Now Routinely Possessed By Third Parties 7

B. Fourth Amendment Principles Should Apply To Personal Information Held By Third Parties In A Manner That Recognizes The Realities Of Americans' Use Of New Technology 15

1. Possession Of An Individual's Personal Information By A Third Party Does Not By Itself Exempt That Information From Fourth Amendment Protection 16

2. Whether A Third Party Obtains Personal Information Through Individuals' "Voluntary" Acts Should Not Be Relevant To The Expectation Of Privacy Inquiry 20

TABLE OF CONTENTS—continued

Page

3. The Legitimate Expectation Of Privacy Inquiry Should Turn On The Nature Of The Personal Information And Whether Individuals Would Reasonably Expect Their Information To Be Generally Available To Others. 23

C. The Cell Phone Location Information Here Is Subject To The Warrant Requirement. 24

1. Location Data Reveals Highly Sensitive Personal Information. 25

2. Individuals Would Not Reasonably Believe That Long-Term Location Data Would Generally Be Available To Third Parties. 29

3. The Warrant Requirement Is Not Burdensome In This Context. 31

4. The Stored Communications Act Standard Does Not Satisfy The Fourth Amendment. 32

CONCLUSION 34

TABLE OF AUTHORITIES

Page(s)

Cases

In re Application of U.S.,
620 F.3d 304 (3d Cir. 2010) 29

Camara v. *Municipal Court*,
387 U.S. 523 (1967) 33

City of Ontario v. *Quon*,
560 U.S. 746 (2010) 1

Commonwealth v. *Augustine*,
4 N.E.3d 846 (Mass. 2014) 25

Katz v. *United States*,
389 U.S. 347 (1967) 4, 16, 17

Kentucky v. *King*,
563 U. S. 452 (2011) 33

Kyllo v. *United States*,
533 U.S. 27 (2001) 5, 6, 16, 28

Minnesota v. *Olson*,
495 U.S. 91 (1990) 16

Missouri v. *McNeeley*,
133 S. Ct. 1552 (2013) 32, 33, 34

Packingham v. *North Carolina*,
137 S. Ct. 1730 (2017) 6

TABLE OF AUTHORITIES—continued

Page(s)

Riley v. *California*,
134 S. Ct. 2473 (2014) ..... *passim*

Smith v. *Maryland*,
442 U.S. 735 (1979) ..... *passim*

Stoner v. *California*,
376 U.S. 483 (1963) 31

United States v. *Jones*,
565 U.S. 400 (2012) ..... *passim*

United States v. *Miller*,
425 U.S. 435 (1976) ..... *passim*

United States v. *Warshak*,
631 F.3d 266 (6th Cir. 2010) 10, 21

Statutes, Rules and Regulations

18 U.S.C. § 2703(a) 33

18 U.S.C. § 2703(b) 33

18 U.S.C. § 2703(c)(1) 32

18 U.S.C. § 2703(d) 32, 33

47 U.S.C. § 222(c)(1) 30

47 U.S.C. § 222(f) 30

47 U.S.C. § 222(h)(1)(A) 30

TABLE OF AUTHORITIES—continued

Page(s)

Other Authorities

Gunes Acar, et al., *The Web Never Forgets* (2014), Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, (pp. 674-689), https://dl.acm.org/citation.cfm?doid=2660267.2660347 14

Kai Biermann, *Betrayed by our own data*, Zeit Online (Mar 10, 2011) 27

Cellular Telecomm. Indus. Ass'n, *Annual Wireless Industry Survey Results* (2017), https://www.ctia.org/docs/default-source/de-fault-document-library/annual-year-end-2016-top-line-survey-results-final.pdf?sfvrsn=2 11

Cellular Telecomm. Indus. Ass'n, *Wireless Snapshot 2017*, https://www.ctia.org/indusrty-data/ctia-annual-wireless-indus-try-survey 22

TABLE OF AUTHORITIES—continued

Page(s)

Deloitte, *Photo sharing: trillions and rising* (2016), https://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/tmt-pred16-telecomm-photo-sharing-trillions-and-rising.html 9

ECPA Reform and the Revolution in Location-Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the House Comm. on the Judiciary, 111th Cong., 25 (2010) (testimony of Prof. Matt Blaze), http://-judiciary.house.gov/_files/hearings/printers/-111th/111-109_5-7082.pdf 12

Fitbit, *Privacy Policy*, https://www.fitbit.com/legal/privacy (last accessed Jul. 25, 2017) 13

Samuel Gibbs, *Jawbone's UP3 fitness device monitors heart rate to track sleep cycles*, The Guardian (Nov. 5, 2014) 13

Google, *Google Maps Geolocation API*, https://-developers.google.com/maps/documentation/geoloca-tion/intro 12

TABLE OF AUTHORITIES—continued

Page(s)

Joseph Hall, *Cell Phone Tracking: Trends in Cell Site Precision* (Apr. 22, 2013), https://www.cdt.org/files/file/cell-location-precision.pdf 10

Chris Jay Hoofnagle, et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 Harvard L. & Policy Review 273 (2012) 14

H.R. Rep. 111-70 (2011) 12

Iron Mountain, Why Cloud Backup: Top 10 Reasons (2010), http://resources.idgenterprise.com/original/AST-0022659_top-_ten_reasons_cloud_backup.pdf 21

Sibren Isaacman et al., *Identifying Important Places in People's Lives from Cellular Network Data* (2011), http://mrm-group.cs.princeton.edu/papers/Isaacman_pervasive11.pdf 27

TABLE OF AUTHORITIES—continued

Page(s)

Kipp Jones, *Skyhook Under the Hood: Determining Location with Wi-Fi Access Points*, Skyhook (Mar. 11, 2015), http://blog.skyhookwireless.com/company/skyhook-under-the-hood-determining-location-with-wi-fi-access-points 13

Dimitris Mavrakis, *Do we really need femtocells?*, SlashData Blog (Dec. 1, 2007), http://www.slashdata.co-/blog/2007/12/do-we-really-need-femnto-cells 11

Steven Melendez, *Nest is Learning to Detect When You're Home*, Fast Company (Mar. 10, 2016), https://www.fastcompany.com/3057706/nest-is-learning-to-detect-when-youre-home 14

Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. Attorneys' Bulletin 16, 19 (2011), http://www.justice.gov/-usao/eousa/foia_reading_room/usab5906.pdf 10

TABLE OF AUTHORITIES—continued

Page(s)

Pew Research Center, Internet/Broadband Fact Sheet (January 2017) 22

Pew Research Center, *Mobile Fact Sheet* (January 2017), http://www.pewinternet.org/fact-sheet/mobile/ 22

Pew Research Center, *Online Shopping and E-Commerce*, http://www.pewinternet.org/2016/12/19/online-shopping-and-e-commerce/ 22

Pew Research Center, *Use of Cloud Computing Applications and Services* (Sept. 2008) 9

Radicati Group, Inc., *Email Statistics Report 2017-2021* (Feb. 2017) 8

Piotr Sapiezynski, et al., *Tracking Human Mobility Using WiFi Signals*, PLoS ONE 10(7) (2015), https://doi.org/10.1371/-journal.pone.0130824 13

Skyhook, *Coverage Area*, http://www.skyhookwireless.com/-Coverage-Map 13

TABLE OF AUTHORITIES—continued

Page(s)

Small Cell Forum, *Small Cells Market Status Report* (2017), http://scf.io/en/whate_papers/Market_status_report_June_2017_Special_edition.php 11

Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 Nw. U.L. Rev. 139 (2016) 29

Eric J. Topol, *The Future of Medicine is in Your Smartphone*, Wall St. J. (Jan. 9, 2015), https://www.wsj.com/articles/the-future-of-medicine-is-in-your-smartphone-1420828632 13

U.S. Dep't of Justice, Retention Periods of Major Cellular Service Providers (Aug. 2010), https://www.aclu.org/files/pdfs/freespeech/retention_periods_of_major_cellular_service_providers.pdf 8

U.S. Postal Service., *A decade of facts and figures* 8

What ISPs Can See, Upturn (Mar. 2016) 14

TABLE OF AUTHORITIES—continued

Page(s)

Fred Zahradnik, *How to Find Your Location History in Google Maps or iPhone* (May 1, 2017)), https://www.-lifewire.com/location-history-google-maps-iphone-1683392 13

En Banc Brief of *Amicus Curiae* AT&T Mobility, LLC in Support of Neither Party, *United States* v. *Davis*, No. 12-12928 (11th Cir. 2014) 10

INTEREST OF THE *AMICUS CURIAE*

The Center for Democracy & Technology (CDT) is a non-profit, public interest organization focused on privacy and other civil liberties issues affecting the Internet, other communications networks, and associated technologies. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

CDT has participated as *amicus curiae* in cases before this Court involving the application of the Fourth Amendment to new technologies, including *Riley* v. *California*, 134 S. Ct. 2473 (2014); *United States* v. *Jones*, 565 U.S. 400 (2012); and *City of Ontario* v. *Quon*, 560 U.S. 746 (2010).[1]

INTRODUCTION AND SUMMARY OF ARGUMENT

This case—like *Riley* v. *California*, 134 S. Ct. 2473 (2014) and *United States* v. *Jones*, 565 U.S. 400 (2012)—brings before the Court an important question regarding the application of the Fourth Amendment in light of the changes wrought by digital technology.

In the pre-digital era, Americans typically stored their personal information at home. Letters, photographs, important documents, health and financial

---

[1] Pursuant to Rule 37.6, *amicus* affirms that no counsel for a party authored this brief in whole or in part and that no person other than *amicus* and its counsel made a monetary contribution to its preparation or submission. The parties' blanket consents to the filing of *amicus* briefs have been filed with the Clerk's office.

information all were printed on paper, which imposed a physical limit on the amount of material that individuals could retain.

Digital technology has transformed the ways that Americans retain their personal information, and also has dramatically altered the quantity and types of personal information that is preserved.

Written letters have largely been replaced by email; and physical documents, photographs, and other records by digital files embodying the same information. This digital data may be stored on an individual's cell phone or laptop computer, but a copy also is likely to be stored "in the cloud" with a third-party service provider.

In addition, third-party service providers collect and retain personal information relating to their customers in the course of providing services to those customers. The cell location information at issue in this case is one example of such information. In addition, fitness and health providers collect and retain detailed information about a customer's physical condition; and Internet browsers retain a record of the websites and individual visits—and that information is accessible by the individual's service provider.

Prior to the widespread adoption of digital technology, this information did not exist because there was no way to gather and preserve it. There was no record of every newspaper, periodical and book that an individual read; or of every location an individual visited; or of a person's minute-by-minute physical condition. Thus, "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical," because govern-

ment officers "would not—and indeed, in the main, simply could not" collect this detailed personal information. *Jones*, 565 U.S. at 429, 430 (Alito, J., concurring in the judgment).

Just as the *Riley* Court took account of the changes wrought by digital technology in applying the search-incident-to-arrest doctrine, the Court in this case must take account of these realities in determining how the Fourth Amendment protects the privacy of highly sensitive personal information in the hands of third parties.

The government argues, and the court below held, that this Court's decisions in *Smith* v. *Maryland*, 442 U.S. 735 (1979), and *United States* v. *Miller*, 425 U.S. 435 (1976), stand for the proposition that personal information in the hands of a third party is not protected by the Fourth Amendment. But neither *Smith* nor *Miller* rested exclusively on the third party's possession of the information—in both cases the Court also discussed the nature of the information at issue.

More fundamentally, there is a vast difference between the narrow types of personal information addressed in *Smith* and *Miller* and the myriad categories and huge amounts of personal information that third parties hold today. For that reason, "any extension of [those cases'] reasoning to digital data has to rest on its own bottom." *Riley*, 134 S. Ct. at 2489.

The changes resulting from digital technology—with Americans storing vast quantities of personal information with third parties, and third parties creating databases of personal information not previously available—make it eminently reasonable to

conclude that Americans have a legitimate expectation of privacy with respect to much of this information. Indeed, holding generally that the Fourth Amendment does not protect an individual's personal information whenever that information is possessed by a third party would—because of these changes—dramatically reduce the protection provided by the Fourth Amendment.

For these reasons, the Court should conclude that the mere fact that personal information is possessed by a third party does not preclude a determination that individuals have an expectation of privacy with respect to that information "that society is prepared to recognize as 'reasonable.'" *Katz* v. *United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

The Court also should recognize that whether the individual provided personal information "voluntarily" should not be accorded any weight in the reasonable-expectation-of-privacy inquiry, because there is no correlation between the voluntary provision of information to a third party and legitimate expectations of privacy. For example, individuals voluntarily transfer the contents of emails, photographs, and sensitive personal documents to third-party service providers who store this information. Yet individuals believe, correctly, that absent very unusual circumstances, this information will be private: it will not be viewed by anyone other than themselves or persons who they authorize. If voluntary provision of information alone precluded Fourth Amendment protection, this highly private information could be obtained by the government without a warrant.

There is a reasonable expectation of privacy in the 127 days of cell site location data at issue here.

Providing a cell phone's location is the equivalent of describing its owner's movements, which is information—like the GPS tracking in *Jones*—that would have been private because the government would not have been able to compile it in the pre-digital era.

Moreover, location information can be combined with other information available to the government to learn about the private aspects of a person's life. Comparing the routes and locations visited by an individual with databases listing the residents, businesses, and other organizations located in those places can reveal religious or political affiliations and other sensitive personal attributes.

The fact that cell phone location data may sometimes be less precise than GPS tracking does not warrant a different result. The relevant comparison is to the information available to the government before the advent of digital technology, and cell location information is dramatically more precise than any tracking that the government would have been able to undertake. In addition, a constitutional rule based on the particular level of precision of the cell phone location information at issue in each case would be wholly impractical. Officers could not know in advance how accurate the information would be and therefore could not anticipate whether a warrant would be required. And courts would face very difficult line-drawing issues.

The circumstances under which third parties acquire and retain cell location data provide further support for a reasonable expectation of privacy. Creation of this data is an unavoidable consequence of using a cell phone, which is a necessity of life in today's world. And a cell service provider's dissemination of this information is strictly limited by federal

and state law. Those facts further enhance the reasonable expectation of privacy.

ARGUMENT

THE FOURTH AMENDMENT'S WARRANT REQUIREMENT APPLIES TO THE CELL PHONE LOCATION DATA AT ISSUE HERE.

The Court has repeatedly recognized that advances in technology must be considered in delineating the Fourth Amendment's protections, because the Court "'must assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *United States* v. *Jones*, 565 U.S. 400, 406 (2012) (quoting *Kyllo* v. *United States*, 533 U.S. 27, 34 (2001)). See also *id.* at 420 (Alito, J., concurring in the judgment) (same); *id.* at 415-418 (Sotomayor, J., concurring) (explaining why changes resulting from technology must be considered in applying the Fourth Amendment); cf. *Packingham* v. *North Carolina*, 137 S. Ct. 1730 (2017) (taking account, in applying the First Amendment, of Americans' use of new mediums of expression resulting from advances in technology).

In *Riley* v. *California*, 134 S. Ct. 2473 (2014), the Court held that the search-incident-to-arrest exception to the warrant requirement did not apply to the contents of cell phones, because digital technology enables the storage in these devices of vast quantities of personal information. "With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.' The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Id.* at 2494-95 (citation omitted).

This case again requires the Court to address the Fourth Amendment's protections in light of the changes resulting from Americans' pervasive use of digital technology.

A. Broad Categories Of Highly Sensitive Personal Information About Virtually Every American Are Now Routinely Possessed By Third Parties.

The pervasive use of digital technology in every facet of life has produced a dramatic change in how Americans store their personal information. Private papers kept in the home have been replaced by digital information stored with third-party service providers. And detailed personal information about individuals that previously could not be collected—because it simply was not possible to do so—is gathered and retained by the third-parties that provide the digital services on which Americans rely.

1. Individuals store a variety of different types of personal information with third-party providers:

- Emails and text messages have displaced physical letters as our principal means of written communication.[2] And both emails and text messages are stored "in the cloud" on computer servers under the control of the

---

[2] U.S. first class mail volume dropped by 50% between 2007 and 2016. U.S. Postal Service, *A decade of facts and figures*, https://about.usps.com/who-we-are/postal-facts/decade-of-facts-and-figures.htm. Email use has grown significantly. *E.g.*, The Radicati Group, Inc., *Email Statistics Report 2017-2021* (Feb. 2017) (projecting 269 billion emails per day worldwide in 2017), http://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf;

service provider.[3] Written letters, by contrast, were stored at home or at another place under the control of the writer or recipient.

- Prior to the advent of digital technology, personal photographs and significant personal documents also were stored in the owner's home. Today, they are likely to be retained in digital, rather than physical, form—and even if they are stored locally in a laptop computer or other device, copies also are stored "in the cloud" on a service provider's server.[4]

---

[3] As the Court explained in *Riley*, 134 S. Ct. at 2491, "'[c]loud computing' is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself"; "users often may not know whether particular information is stored on the device or [on a server], and it generally makes little difference." For example, the contents of "gmail" email accounts are stored on servers controlled by Google; "hotmail" accounts on servers controlled by Microsoft; and "yahoo" accounts on servers controlled by that company. Storage of text messages varies by service provider: some providers do not retain copies of text messages. Others store messages for a limited period of time. U.S. Dep't of Justice, Retention Periods of Major Cellular Service Providers (Aug. 2010), https://www.aclu.org/files/pdfs/freespeech/retention_periods_of_major_cellular_service_providers.pdf.

[4] See note 3, *supra*; see also Pew Research Center, *Use of Cloud Computing Applications and Services* (Sept. 2008), http://www.pewinternet.org-/2008/09/12/use-of-cloud-computing-applications-and-services/; Deloitte, *Photo sharing: trillions and rising* (2016) ("2.5 trillion photos will be shared or stored online"), https://www2.deloitte.com/global/en/-pages/technology-media-and-telecommunications/articles/tmt-pred16-telecomm-photo-sharing-trillions-and-rising.html.

- The same is true of individuals' health and financial information. Records that formerly were kept in physical form at home are now likely to be digital, and stored remotely with service providers whether or not copies of the digital records are also stored locally. This information may be stored in the form of emails or email attachments; or as digital documents; or it may be stored with the company providing mobile application services ("apps") for which the information is relevant, such as a health or financial services. (And, as the Court observed in *Riley*, the more than one million apps extend far beyond health and finance to cover every conceivable need and interest—from politics, to addiction treatment, to romance and shopping. 134 S. Ct. at 2490. Each app collects and stores information relevant to the service it provides.).

Importantly, most service providers retain the right to access digital information stored in the cloud by their customers.[5] All of this highly personal information in the custody of third parties is therefore also accessible by those third parties.

2. Third-party digital service providers themselves collect and retain additional personal information relating to their customers in the course of providing services to those customers.

The cell site location information ("cell location information" or "CSLI") at issue in this case is one

---

[5] *E.g.*, *United States* v. *Warshak*, 631 F.3d 266, 286 (6th Cir. 2010).

example. As petitioner explains (Br. 3-4), cell phones access the telecommunications network by connecting to cell towers (also called "cell sites"). Each tower has several directional antennas that divide the covered area into sectors. The cellular service provider maintains a record of the tower and antenna with which a cellphone connects. Because the service provider typically knows the precise latitude and longitude of its cell towers, this data can be used to locate a user within the particular cell served by that tower and within a particular sector of that cell.[6]

CSLI's precision in pinpointing a cell phone's location depends on the size of the area served by the tower, the number of directional antennas on the tower (which determine the number of sectors), and the technology deployed on the cell tower.[7] In the last ten years, the number of cell sites has increased by 57%—a trend that is expected to continue.[8] And new technology is further improving the precision of cell location information.[9]

---

[6] Joseph Hall, *Cell Phone Tracking: Trends in Cell Site Precision* (Apr. 22, 2013), https://www.cdt.org/files/file/cell-location-precision.pdf; En Banc Brief of *Amicus Curiae* AT&T Mobility, LLC in Support of Neither Party, *United States* v. *Davis*, No. 12-12928 (11th Cir. 2014); Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. Attorneys' Bulletin 16, 19 (2011), http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf.

[7] See generally Hall, *supra* note 6.

[8] Cellular Telecomm. Indus. Ass'n, *Annual Wireless Industry Survey Results* (2017), https://www.ctia.org/docs/default-source/de-fault-document-library/annual-year-end-2016-top-line-survey-results-final.pdf?sfvrsn=2.

[9] Wireless providers have been augmenting their networks with many smaller cells, each with its own antenna. The areas

More, smaller cell sites with improved technology means more accurate location information--approaching or even exceeding the precision of the location information provided by the Global Position System tracking process before the Court in *Jones*. See 565 U.S. at 403 (50-100 feet, which equals 15-30 meters). Thus, "[w]hile it is still the case in rural areas that location derived from cell phone antennas is not comparable to GPS (10 meters), in a growing number of cases, especially in urban areas, location based on antenna location will approach GPS-level precision."[10]

---

served by these new cells are much smaller than those served by traditional cell towers, resulting in increased location precision. See Small Cell Forum, *Small Cells Market Status Report* at 4, Tables 2-2, 2-3 (2017), http://scf.io/en/whate_papers/ Market status report June 2017 Special edition.php (reporting that Industry analysts expect new small cell shipments in North America to exceed 290,000 in 2017, and to increase to over 550,000 by 2020); see generally Hall, *supra* note 6, at 5.

These small cells are called "microcells," "picocells" and "femtocells." The exact specifications for each term vary, but according to one source, microcells, picocells and femtocells provide service to areas of 200m-2km, 4m-200m, and 10m respectively. Dimitris Mavrakis, *Do we really need femtocells?*, SlashData Blog (Dec. 1, 2007), http://www.slashdata.co-/blog/2007/12/do-we-really-need-femto-cells.

[10] Hall, *supra* note 6, at 2. A 2011 report of the House Judiciary Committee summarized testimony before the committee explaining that "the precision of [cell location data] will vary widely for any given customer of the course of a day and, for a typical user over time, some of that data will likely have locational precision similar to that of GPS. Indeed, in urban areas where providers are using microcell technology, the level of precision for cell tower location data can include individual floors and rooms within buildings." H.R. Rep. 111-70, at 90 (2011); see also *ECPA Reform and the Revolution in Location-Based Technologies and Services: Hearing Before the Subcomm. on the*

Other service providers collect and retain detailed data regarding their customers' movements. Virtually every smartphone today contains a "map" feature that enables the user to find her location and obtain directions for reaching a specified destination. These features use cell site location data combined with data about WiFi access points to identify the user's location, and maintain a record of that location information.[11]

Service providers collect and retain many other types of personal information. For example:

Constitution, Civil Rights, and Civil Liberties of the House Comm. on the Judiciary, 111th Cong., 25 (2010) (testimony of Prof. Matt Blaze), http://judiciary.house.gov/_files /hearings/printers/-111th/111-109_5-7082.pdf.

[11] For example, the Google Maps Geolocation function returns location information based on data about nearby cell towers and WiFi access points. Google, *Google Maps Geolocation API*, https://-developers.google.com/maps/documentation/geolocation/intro. When a mobile device searches for a WiFi connection, it collects information about nearby WiFi access points. By recording the relative strength of WiFi signals, a device's location can be pinpointed based on the physical location of the WiFi access points stored in the database. *See, e.g.*, Skyhook, *Coverage Area*, http://www.skyhookwireless.com/-Coverage-Map; Kipp Jones, *Skyhook Under the Hood: Determining Location with Wi-Fi Access Points*, Skyhook (Mar. 11, 2015), http://blog.skyhookwireless.com/company/skyhook-under-the-hood-determining-location-with-wi-fi-access-points. See also Piotr Sapiezynski, et al., *Tracking Human Mobility Using WiFi Signals*, PLoS ONE 10(7) (2015), https://doi.org/10.1371/-journal.pone.0130824. These mapping features store the user's location information unless the user turns off the storage feature. Fred Zahradnik, *How to Find Your Location History in Google Maps or iPhone* (May 1, 2017), https://www.-lifewire.com/location-history-google-maps-iphone-1683392.

- Devices such as the Fitbit, which help users maintain physical fitness regimes, collect the user's heart rate, steps taken, and sleeping patterns.[12] Cell phones can be used to transmit medical information to doctors in real time.[13]
- Many individuals use services employing digital technology to control remotely home thermostats, smoke alarms, and other devices, as well as cameras to enable them to monitor their home's condition. These services record a variety of data, including when the home is occupied.[14]
- An individual's Internet browser retains a record of the websites that the individual visits—and much of that data is accessible by the individual's internet service provider.[15] Online advertisers deposit "cookies" in indi-

---

[12] Samuel Gibbs, *Jawbone's UP3 fitness device monitors heart rate to track sleep cycles*, The Guardian (Nov. 5, 2014); *Privacy Policy*, Fitbit, https://www.fitbit.com/legal/privacy (last accessed Jul. 25, 2017) ("When you use [the Fitbit], we collect data like number of steps you take or your [Body Mass Index] to show your stats and progress. And when you sync, we collect data like sync time and battery level, to help you keep your tracker (and yourself) up and running.").

[13] Eric J. Topol, *The Future of Medicine is in Your Smartphone*, Wall St. J. (Jan. 9, 2015), https://www.wsj.com/articles/the-future-of-medicine-is-in-your-smartphone-1420828632.

[14] Steven Melendez, *Nest is Learning to Detect When You're Home*, Fast Company (Mar. 10, 2016), https://www.fastcompany.com/3057706/nest-is-learning-to-detect-when-youre-home.

[15] *What ISPs Can See*, Upturn (Mar. 2016), https://www.teamupturn.com/reports/2016/what-isps-can-see.

viduals' Internet browsers that can be used to record the websites an individual visits.[16]

Prior to the invention and widespread use of digital technology, these detailed collections of highly personal information did not exist. Cf. *Jones*, 565 U.S. at 429, 430 (Alito, J., concurring in the judgment) (recognizing that "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical"; and explaining that government officers "would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period").

In sum, digital technology has produced dramatic changes in the ways that Americans preserve their personal information and in the amount of personal information that is available. Those changes largely parallel the characteristics of cell phones described by the Court in *Riley*:

- The sheer amount of information is enormous—much more than any American could physically retain in the pre-digital era. Indeed, cloud computing allows the storage of limitless amounts of information, unlike a single cell phone which has a finite storage capacity.

---

[16] Chris Jay Hoofnagle, et al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 Harvard L. & Policy Review 273 (2012); Gunes Acar, et al., *The Web Never Forgets* (2014), Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 674-689), https://dl.acm.org/citation.cfm?doid=2660267.2660347.

- The information is virtually always stored outside the home and in the custody of third parties—on servers "in the cloud."
- "[T]here is an element of pervasiveness that characterizes [digital data] but not physical records." *Riley*, 134 S. Ct. at 2490. As discussed above, the personal information held by third parties encompasses every aspect of an individual's life.

Just as the *Riley* Court took account of the changes wrought by digital technology in applying the search-incident-to-arrest doctrine, the Court in this case must take account of these realities in determining how the Fourth Amendment protects the privacy of highly sensitive personal information in the hands of third parties.

B. Fourth Amendment Principles Should Apply To Personal Information Held By Third Parties In A Manner That Recognizes The Realities Of Americans' Use Of New Technology.

A search within the meaning of the Fourth Amendment occurs when the government's conduct encroaches on an expectation of privacy "that society is prepared to recognize as 'reasonable.'" *Katz* v. *United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); see also *Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment); *id.* at 415 (Sotomayor, J., concurring); *Kyllo*, 533 U.S. at 33. That inquiry looks to the privacy expectations of "the hypothetical reasonable person"—"the average person's [privacy] expectations." *Jones*, 565 U.S. at 427, 429 (Alito, J., concurring); see also *Minnesota* v. *Olson*, 495 U.S.

91, 98 (1990) ("the every-day expectations of privacy that we all share").

The fact that an individual's personal information is held by a third party does not preempt this inquiry. This Court's precedents from the pre-digital era do not hold that a third party's possession of an individual's personal data by itself precludes a reasonable expectation of privacy with respect to that information. And the changes resulting from digital technology—with Americans storing vast quantities of personal information with third parties, and third parties creating databases of personal information not previously available—make it eminently reasonable to conclude that Americans have a legitimate expectation of privacy with respect to much of this information.

The circumstances surrounding the third party's acquisition and possession of the data may of course be relevant to the *Katz* inquiry. But the possession of information by a third party is not dispositive of the critical inquiry, which remains whether there is a reasonable expectation of privacy with respect to the information sought by the government.

1. *Possession Of An Individual's Personal Information By A Third Party Does Not By Itself Exempt That Information From Fourth Amendment Protection.*

The court below concluded that this case involves "business records obtained from a third party," and that the Court's decisions in *Smith* v. *Maryland*, 442 U.S. 735 (1979), and *United States* v. *Miller*, 425 U.S. 435 (1976), establish that petitioner could not have a reasonable expectation of privacy in the information contained in those records. Pet. App. 14a. That con-

clusion is wrong. Possession of an individual's personal information by a third party does not automatically preclude Fourth Amendment protection.

Neither *Smith* nor *Miller* rested exclusively on the third party's possession of the information—in both cases the Court also discussed the nature of the information at issue. The checks in *Miller* were "not confidential communications but negotiable instruments to be used in commercial transactions"; and both checks and deposit slips contain information "exposed to [banks'] employees in the ordinary course of business." 425 U.S. at 442. With respect to the dialed telephone numbers collected by the pen register at issue in *Smith*, the Court "doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial," because they knew that the numbers were used to route calls, were recorded by the company, and were used by the company for a variety of purposes. 442 U.S. at 742.

To be sure, both opinions contain broad language referring to the lack of a legitimate expectation of privacy in information conveyed to third parties. *E.g.*, *Smith*, 442 U.S. at 743-44. But neither holding rested exclusively on that ground; each expressly addressed and relied on the particular nature of the information that was conveyed.

There is a vast difference between the narrow types of personal information addressed in *Smith* and *Miller* and the myriad categories and huge amounts of personal information that third parties hold today. See pages 7-15, *supra*. For that reason, "any extension of [those cases'] reasoning to digital data has to rest on its own bottom." *Riley*, 134 S. Ct. at 2489.

The Court should not extend *Smith* and *Miller* to this very different context. Holding generally that the Fourth Amendment does not protect an individual's personal information whenever that information is possessed by a third party would dramatically reduce the protection provided by the Fourth Amendment.

First, much of the information today held by third parties formerly was stored in an individual's home—such as private communications, pictures and documents containing personal information, and medical and financial information. To gain access to that information before the advent of digital technology, the government had to obtain a warrant. Holding that the Fourth Amendment does not apply if the information is in the hands of a third party would therefore eliminate the constitutional protection for this information, and very substantially reduce the protection for Americans' privacy.

Second, the detailed personal information generated in connection with services provided by third parties—an individual's location, everything she reads on the Internet, and her health data, to cite just a few examples—was not previously available to the government because it did not exist. There was no record of every newspaper, periodical and book that an individual read; or of every location an individual visited; or of a person's minute-by-minute physical condition. Permitting the government to obtain this information without a warrant would also therefore significantly diminish privacy protection. Accord, *Jones*, 565 U.S. at 428-30 (Alito, J., concur-

ring in the judgment); *id.* at 415-17 (Sotomayor, J., concurring).[17]

The *Riley* Court's observation with respect to the search of a cell phone's contents thus applies fully to a search by the government of personal data possessed by third parties: it would "typically expose to the government far more than the most exhaustive search of a house," because third parties "not only [possess] in digital form many sensitive records previously found in the home; [they] also [possess] a broad array of private information never found in a home in any form." 134 S. Ct. at 2491.

The government asserts that *Smith* and *Miller* stand for the broad principle that an individual can never have a reasonable expectation of privacy in information contained in a third party's "business records." Opp. 11-12. That is no limiting principle, however, because the term "business records" has no fixed meaning and therefore provides no guidance as to what types of information possessed by a business qualify as a "business record" and what types do not.

Indeed, the government argues in a related context that the contents of emails stored with an email service provider qualify as the provider's "business records." Pet. for a Writ of Cert. at 23-24, *United States* v. *Microsoft Corp.*, No. 17-2 (U.S. June 23,

---

[17] The government invokes (Opp. 24-25) the Stored Communications Act in arguing that Congress has provided appropriate privacy protection in this context. But that statute—enacted in 1986 and amended in 1994—preceded the sea change in Americans' use of third-party service providers. It therefore could not embody any determination with respect to the appropriate privacy protection in this dramatically different context. See pages 32-33, *infra*.

2017) (asserting that email contents constitute the service provider's business records and therefore must be produced pursuant to a subpoena served in the United States even if stored outside the United States). The government's rule therefore would sweep in all personal information in the possession of a third party—and therefore would result in the same very substantial reduction in Fourth Amendment protection.

2. Whether A Third Party Obtains Personal Information Through Individuals' "Voluntary" Acts Should Not Be Relevant To The Expectation Of Privacy Inquiry.

The Court's opinions in *Smith* and *Miller* observe that the information at issue in those cases was "voluntarily" provided to the telephone company and to the bank respectively. See 442 U.S. at 743-44; 425 U.S. at 442. Petitioner (Br. 39-44) and the government (Opp. 15-17) debate whether the location information at issue here was provided voluntarily or involuntarily.

Given the realities of today's digital environment, whether an individual provides information voluntarily should not be accorded any weight in the reasonable-expectation-of-privacy inquiry.

There simply is no correlation between the voluntary provision of information to a third party and legitimate expectations of privacy. Individuals voluntarily transfer the contents of emails, photographs, and sensitive personal documents to third-party service providers who store this information. Yet individuals believe, correctly, that absent unusual circumstances, this information will be private: it will not be viewed by anyone other than themselves or

persons who they authorize.[18] If voluntary provision of information alone precluded Fourth Amendment protection, this highly private information could be obtained by the government without a warrant.

Indeed, as the Court observed in *Riley*, individuals "often may not know" whether information is stored on their devices or on remote servers. 134 S. Ct. at 2491. And most experts advise individuals to store information remotely so that a problem with a cell phone, laptop, or other device will not mean that information will be permanently unavailable.[19]

Moreover, if voluntariness were somehow relevant, there can be no serious argument that the use of these services is any sense voluntary in today's world. Email services and a wide variety of other applications that encompass sensitive personal information are accessed via cell phones—and cell phones and the services they provide are now, as the Court recognized in *Riley*, "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude that they were an important feature of human anatomy." 134 S. Ct at 2484.

Data confirms the pervasiveness of Americans' use of these services: 95% own a cell phone of some type and 77% own smart phones; 80% of adults own laptop computers; and 50% of adults own tablet com-

---

[18] Although service providers retain the right to review emails, documents, and other materials stored with them, that right is limited and in reality virtually never takes place—and therefore does not diminish users' reasonable expectation of privacy. See, e.g., *United States* v. *Warshak*, 631 F.3d at 286-88.

[19] Iron Mountain, Why Cloud Backup: Top 10 Reasons (2010), http://resources.idgenterprise.com/original/AST-0022659_top-_ten_reasons_cloud_backup.pdf

puters.[20] Nine-in-ten adults use the Internet; three-quarters have broadband service at home; and 80% shop on-line.[21] Americans spend an average of two and one half hours each day using Internet-based applications on their cell phones or accessing the Internet using their cell phones.[22] And "[t]he average smart phone user has installed 33 apps."[23] Utilizing these services is not voluntary—it is a necessity of modern life.

Finally, while "voluntarily" providing sensitive personal information to a third party should not preclude Fourth Amendment protection because of the changes in American's behavior and expectations resulting from digital technology, but involuntarily providing information should be a factor favoring such protection. If an individual does not know that she has imparted personal information, the fact that the information is in the possession of a third party should not be relevant to the Fourth Amendment inquiry—the individual's reasonable expectation of privacy would be the same as if the information had remained in her possession.

---

[20] Pew Research Center, *Mobile Fact Sheet* (January 2017), http://www.pewinternet.org/fact-sheet/mobile/.

[21] Pew Research Center, Internet/Broadband Fact Sheet (January 2017), http://www.pewinternet.org/fact-sheet/internet-broadband/; Pew Research Center, *Online Shopping and E-Commerce*, http://www.pewinternet.org/2016/12/19/online-shopping-and-e-commerce/.

[22] Cellular Telecomm. Indus. Ass'n, *Wireless Snapshot 2017*, https://www.ctia.org/industry-data/ctia-annual-wireless-industry-survey.

[23] *Riley*, 134 S. Ct. at 2490.

3. *The Legitimate Expectation Of Privacy Inquiry Should Turn On The Nature Of The Personal Information And Whether Individuals Would Reasonably Expect Their Information To Be Generally Available To Others.*

The focus of the Fourth Amendment inquiry in the context of personal information in the possession of a third party should be no different than in other contexts: the question is whether the individual has a reasonable expectation of privacy with respect to that information.

Two basic factors are relevant.

The nature of the information sought. A court should assess whether the data sought encompasses sensitive personal information as to which there is a reasonable expectation of privacy. That inquiry would take account of the nature of the data, the volume sought, and what it would reveal about an individual—both alone and when combined with other information available to law enforcement officers.

The latter inquiry is particularly important. Digital technology enables the government to combine datasets with relative ease. Such cross-matching may reveal more personal information than each dataset standing alone. To take one elementary example, cross-matching information about an individual's movements with the businesses or individuals resident at the places that she stops could reveal extremely sensitive information. Repeated visits to an oncologist could reveal a health condition; visits to a political party office or other organization could reveal political or policy views.

But data matching can be much more sophisticated. Integrating even some of the numerous datasets in the hands of third parties could enable the government to learn many private details about a person's life. Cf. *Riley*, 134 S. Ct. at 2490 (the apps on an individual's smartphone "together can form a revealing montage of the user's life").

The circumstances under which the information was provided to the third party. A court should assess societal expectations regarding the general availability to others of the particular information provided to or obtained by the third party. That would include whether the information is subject to contractual, regulatory, statutory, or judicial limits on its dissemination by the third party. If the information was obtained involuntarily, that fact should weigh in favor of a reasonable expectation of privacy.

C. The Cell Phone Location Information Here Is Subject To The Warrant Requirement.

There is a reasonable expectation of privacy in 127 days of cell site location data showing the location of petitioner's cell phone during that period. Like the GPS tracking data at issue in *United States* v. *Jones*, this information was private prior to the advent of digital technology, because there was no way to collect it. Moreover, such detailed location data allows law enforcement officers to obtain extremely sensitive information about the most personal aspects of an individual's life. Finally, the circumstances under which the information was obtained, and the legal regime governing the third party's treatment of the information, confirm that there is a reasonable expectation in the information's privacy.

1. Location Data Reveals Highly Sensitive Personal Information.

The long-term cell phone location data obtained by the government is extremely sensitive information in which individuals have a reasonable expectation of privacy.

First, there is no doubt that data providing a cell phone's location for 127 days is the equivalent of information describing all of its owner's movements during that period. Indeed, the movements of a cell phone are more likely to parallel its owner's location than the movements of the car in *Jones*—individuals often park a car and walk to a different location, or series of locations, but it is rare indeed for an individual to be separated from her cell phone. *Riley*, 134 S. Ct. at 2490 (stating that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower"); see also *Commonwealth* v. *Augustine*, 4 N.E.3d 846, 861 (Mass. 2014) (observing that "because a cellular telephone is carried on the person of its user, it tracks the user's location far beyond the limitations of where a car can travel").

Second, the tracking of the phone, like the GPS tracking in *Jones*, provides a record of an individual's movements that law enforcement officers would not have been able to compile in the pre-digital era. To come close "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance." *Jones*, 565 U.S. at 429 (Alito, J., concurring in the judgment) (footnote omitted).

And the task of tracking an individual would be much more difficult than tracking a vehicle—because

individuals are smaller and therefore harder to identify from afar; they more easily blend in with a crowd; and they can walk in and out of buildings, make sudden changes in their route, and take other actions that make tracking difficult. Therefore, it is even more true in this context that with respect to routine law enforcement investigations such as the robbery investigation here, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's [phone] for a very long period." *Id.* at 430.

The court below found no reasonable expectation of privacy in the cell location data here in part because it determined that the cell location data was less precise than the GPS tracking data in *Jones*. Pet. App. 12a-14a. That conclusion is wrong for several reasons.

To begin with, even though cell location data may sometimes be less precise than GPS tracking, it is dramatically more precise than the information available to the government before the advent of digital technology—and that is the relevant comparison. Without digital technology, the government could not have compiled a 127-day record of petitioner's movements. And the fact that the government uses the data in court to place a defendant at the scene of criminal activity (See Pet. Br. 24-26) confirms that the information it provides is sufficiently precise to infringe on reasonable privacy expectations.

Moreover, the precision of cell location data varies based on the size of the cell, the number of antennas on the cell tower, and the particular technology used by the cell. In many urban areas, cell loca-

tion information today is just as precise as GPS information. As the number of cell towers increases, and new technology is deployed, GPS-level precision will be available broadly. See pages 9-11, *supra*.

In addition, long-term location data does not just infringe on the reasonable expectation that our daily movements will not be tracked by the government; it also enables the government to learn about the private aspects of a person's life. That is true of cell location information generally, which can be analyzed to determine particular locations and routes important to the individual.[24] Analysis of those locations and routes in turn can reveal religious affiliation, political affiliation, and other sensitive personal attributes.[25]

When cell location information approaches the accuracy of GPS tracking—as it increasingly does today—then it can reveal "a wealth of detail about [an individual's] familial, political, professional, religious, and sexual associations." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

Third, a constitutional test should not turn on the particular level of precision of the cell location data in this case. See *Kyllo*, 533 U.S. at 36 (observing that although "the technology used in the [case before the Court] was relatively crude, the rule we

---

[24] Sibren Isaacman et al., *Identifying Important Places in People's Lives from Cellular Network Data* (2011), http://mrm-group.cs.princeton.edu/papers/Isaacman_pervasive11.pdf.

[25] *E.g.*, Kai Biermann, *Betrayed by our own data*, Zeit Online (Mar 10, 2011) (personal information obtained when German Parliament member allowed newspaper to obtain his cell location data for one week), http://www.zeit.-de/digital/datenschutz/2011-03/data-protection-malte-spitz.

adopt must take account of more sophisticated systems that are already in use or in development").

Such a rule would be completely impractical. Officers could not know in advance where a particular individual had traveled or the particular level of precision of the cell site information in each of those areas. They accordingly would not know in advance whether the location information they would obtain with respect to their target would be at "GPS-level" or a lesser level of precision. The officers accordingly could not know in advance whether or not Fourth Amendment protection would be triggered.

Courts would be faced with difficult line-drawing issues. They would have to assess the level of precision in each of the cells at issue. Then they would have to determine whether the particular level of precision triggers the Fourth Amendment.

The *Riley* Court's rationale for rejecting a similarly vague test—permitting searches of cell phone contents where the information could have been obtained from a pre-digital source—is fully applicable to a level-of-geographic precision test for cell location information. Such a test "would launch courts on a difficult line-drawing expedition to determine which [cell location information is] comparable to [GPS information]. * * * It is not clear how officers could make these kinds of decisions before conducting a search, or how courts would apply the proposed test after the fact. [The] test would 'keep defendants and judges guessing for years to come.'" 134 S. Ct. at 2493 (citation omitted).

2. *Individuals Would Not Reasonably Believe That Long-Term Location Data Would Generally Be Available To Third Parties.*

The 127 days of location data relating to petitioner was held by third parties. It therefore is necessary to assess whether the circumstances under which the third parties acquired and retained the data undermine a reasonable expectation of privacy. They do not.

Creation of this data is an unavoidable consequence of using a cell phone. To the extent an individual wishes to have a cell phone—a necessity of life in today's world (see pages 21-22, *supra*)—location information will be collected and stored by the service provider. Whether or not a user knows that this takes place, and many, perhaps most, almost certainly do not,[26] the user has no choice.

Importantly, a cell service provider's dissemination of cell location information is strictly controlled. Federal law bars its disclosure without the customer's approval unless otherwise authorized by law. 47 U.S.C. § 222(c)(1), (f), (h)(1)(A). A number of States require law enforcement officers to obtain a warrant

---

[26] Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 Nw. U.L. Rev. 139, 177 (2016) (survey participants "were asked whether their cell phone service provider regularly collects information on their physical location using their cell phone. Nearly three-quarters of participants (73.5%) answered either 'No' (15.0%) or 'I Don't Know') (58.5%)"); see also *In re Application of U.S.*, 620 F.3d 304, 317 (3d Cir. 2010) (observing that "it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store" location information).

in order to access this information. Pet. Br. 22-23. These protections strongly support a reasonable expectation that the information would remain private.

The fact that the location information is possessed and accessed by a third party does not by itself vitiate the reasonable expectation of privacy. We already have explained why precluding Fourth Amendment protection for any information possessed by a third party would effect a very substantial reduction in Americans' privacy protection in light of the huge amount of personal information held by third parties due to the advent of digital technology. See pages 7-15, *supra*. The same result would follow from a rule withdrawing Fourth Amendment protection because the third party is authorized to access the information.

The Court has never endorsed the principle that an individual's decision to place information in a location in which it might be observed by another—or even to share private information with someone—vitiates a reasonable expectation of privacy in that information. Inviting guests into one's home does not relieve the government of its obligation to obtain a warrant, even if the information sought was in plain view of the guests.

Similarly, leaving private information in a hotel room—which is also accessible by the hotel owner—does not vitiate the expectation of privacy in that information. *Stoner* v. *California*, 376 U.S. 483 (1963). And the same is true of material placed in a safe deposit box, even though the bank has the ability and legal right to access the box on its own.

So too here. The ability of a cell service provider—or an email service provider, or the provider of

any of a myriad other digital services—to access the user's personal information under limited circumstances supports, rather than diminishes, the reasonable expectation of privacy with respect to that information.

This is not a situation in which an individual uses a digital medium to publish personal information to the world generally, or to a large group of individuals, or provides the information to a third party with knowledge that the third party will distribute it generally. To the contrary, the information here was generated as a consequence of using an essential service, and the use and distribution of the information is tightly restricted. Those facts enhance, rather than diminish, the reasonable expectation of privacy.

3. The Warrant Requirement Is Not Burdensome In This Context.

The Court has recognized that "the warrant requirement is 'an important working part of our machinery of government,' not merely an inconvenience to be somehow 'weighed' against the claims of police efficiency." *Riley*, 134 S. Ct. 2493 (citation omitted). Here, moreover, the warrant requirement will not impose any significant burden.

As the Court has noted, technological advances have "made the process of obtaining a warrant itself more efficient." *Ibid.*; see also *Missouri* v. *McNeeley*, 133 S. Ct. 1552, 1561-63 (2013).

Most importantly, the Stored Communications Act requires government officers to apply for judicial authorization to obtain cell location information without the customer's consent. 18 U.S.C. § 2703(c)(1). They may obtain either a warrant, or an

order based on a finding that "specific and articulable facts" show "reasonable grounds to believe that [the information sought is] relevant and material to an ongoing criminal investigation." *Id.* § 2703(d).

Because government officers already are obligated to obtain judicial process, requiring a warrant does not impose any additional procedural burden.

4. The Stored Communications Act Standard Does Not Satisfy The Fourth Amendment.

The government argues that the Stored Communications Act standard for government access to this information should control here—either because Congress made a determination to which the Court should defer, or because that standard satisfies the "reasonableness" requirement of the Fourth Amendment. Opp. 23-26. The government is wrong on both counts.

The congressional determinations embodied in the Act were made before digital devices became an essential part of Americans' everyday lives. The statute was enacted in 1986; and the government access provisions were last substantively amended in 1994. As petitioner explains (Pet. Br. 50), in 1986 few Americans owned cell phones and there were dramatically fewer cell towers—making cell location information both less of an issue for law enforcement and much less accurate. Congress could not have been focused on this issue when it enacted these statutory provisions.

Other provisions of the Act confirm this conclusion. To take just one example, the Act permits the government to obtain the contents of emails stored for longer than 180 days without obtaining a war-

rant; the government may use an administrative subpoena or a court order based on "reasonable grounds to believe" that the information is relevant to an investigation. 18 U.S.C. § 2703(a), (b), (d). Surely Congress did not—and could not reasonably—determine that Americans' privacy interest in emails, documents, and photographs automatically diminishes after 180 days. Rather Congress at the time did not, and could not, anticipate the revolution in the ways Americans retain personal information that has resulted from the pervasive use of digital technology.

The argument for an exception to the warrant requirement is similarly flawed. The Fourth Amendment's general requirement is that the law enforcement officers obtain a warrant, supported by probable cause, to conduct a search. "[E]xcept in certain carefully defined classes of cases, a search of private property without proper consent is 'unreasonable unless it has been authorized by a valid search warrant." *Camara* v. *Municipal Court*, 387 U.S. 523, 528-29 (1967); see also *McNeely*, 133 S. Ct. at 1558; *Kentucky* v. *King*, 563 U. S. 452, 459 (2011). An exception to this rule must be justified by special circumstances.

There are no such circumstances here. Federal law already requires recourse to a court, and exceptions to the warrant requirement generally turn upon the special burden on law enforcement that would result from requiring judicial intervention in particular circumstances. *McNeely*, 133 S. Ct. at 1559. Because officers already must obtain a court order, and the only question is the standard they must satisfy to obtain that order, there is no basis for creating a new exception to the warrant requirement here.

CONCLUSION

The judgment of the court of appeals should be reversed.

Respectfully submitted.

ANDREW J. PINCUS
Counsel of Record
Mayer Brown LLP
1999 K Street, NW
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com

Counsel for Amicus Curiae

AUGUST 2017

RECORD AND BRIEFS

No. 16-402

FILED
AUG 11 2017
OFFICE OF THE CLERK
SUPREME COURT, U.S.

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Sixth Circuit

BRIEF FOR THE COMPETITIVE ENTERPRISE INSTITUTE, CATO INSTITUTE, REASON FOUNDATION, AND COMMITTEE FOR JUSTICE AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

Ilya Shapiro
CATO INSTITUTE
1000 Mass. Ave. N.W.
Washington, D.C. 20001
(202) 842-0200
ishapiro@cato.org

Manuel S. Klausner
LAW OFFICES OF MANUEL S. KLAUSNER
One Bunker Hill Building
601 W. Fifth St., Suite 800
Los Angeles, CA 90071
(213) 617-0414
mklausner@klausnerlaw.us

Jim Harper
Counsel of Record
Ryan C. Radia
COMPETITIVE ENTERPRISE INSTITUTE
1310 L St. NW, 7th Floor
Washington, D.C. 20005
(202) 331-1010
jim.harper@cei.org

Curt Levey
The Committee for Justice
722 12th St. NW, 4th Floor
Washington, DC 20005
(202) 270-7748
clevey@committeeforjustice.org

August 11, 2017

QUESTION PRESENTED

Can the government seize and review anyone's cell-site location data– which reveals all of their movements over extended periods—without a warrant?

TABLE OF CONTENTS

QUESTION PRESENTED i

TABLE OF AUTHORITIES iv

INTEREST OF *AMICUS CURIAE* 1

INTRODUCTION AND SUMMARY OF ARGUMENT 2

ARGUMENT 4

I. THIS COURT SHOULD APPLY THE TERMS OF THE FOURTH AMENDMENT IN ALL FOURTH AMENDMENT CASES 4

II. THIS COURT SHOULD ESCHEW THE UNSOUND "REASONABLE EXPECTATION OF PRIVACY" TEST AND OTHER UNHELPFUL DOCTRINES 8

A. *Ex Parte Jackson* Properly Protected Communications in Transit by Protecting Papers and Effects as Such 9

B. *Olmstead* Involved Seizures and Searches of a Wire and Electronic Papers/Effects 10

C. The *Katz* Majority Inarticulately Applied the Fourth Amendment's Terms to a Shrouded Oral Communication 12

D. The Ills of the "Reasonable Expectation of Privacy" Test 13

E. Corollaries of the "Reasonable Expectation of Privacy" Test Are Even Worse 15

III. THIS COURT'S RECENT CASES ARE A FRAMEWORK FOR ADMINISTERING THE FOURTH AMENDMENT IN A RELIABLE AND JURIDICAL WAY 19

A. *Jones* Was a Seizure Case 19

B. *Kyllo* Is a High-Tech Search Case 20

C. "Papers" and "Effects" Can Take a Digital Form 22

IV. THE GOVERNMENT SEIZED AND SEARCHED PETITIONER'S DIGITAL PAPERS, WHICH WAS UNREASONABLE WITHOUT A WARRANT 25

A. There Was a Seizure 25

B. There Was a Search 26

C. "Papers" or "Effects" Were Involved 27

D. Carpenter and Sanders Owned Them 28

E. The Government's Actions Were Unreasonable 32

CONCLUSION 34

TABLE OF AUTHORITIES

Cases **Page(s)**

ACLU v. Clapper,
785 F.3d 787 (2d Cir. 2015) 19

Boyd v. United States,
116 U.S. 616 (1886) 23

Brendlin v. California,
551 U.S. 249 (2007) 6

California Bankers Ass'n v. Shultz,
416 U.S. 21 (1974) 16

Chimel v. California,
395 U.S. 752 (1969) 6, 31

Dolan v. City of Tigard,
512 U.S. 374 (1994) 25

In re Facebook Internet Tracking Litigation,
No. 5:12-md-02314-EJD (N.D. Cal. filed Feb. 8, 2012) 29

Ex Parte Jackson,
96 U.S. 727 (1878) 8, 9, 10, 12

Horton v. California,
496 U.S. 128 (1990) 9

Illinois v. Caballes,
543 U.S. 405 (2005) 15

Illinois v. Lafayette,
462 U.S. 640 (1983) 7

Kaiser Aetna v. United States,
444 U.S. 164 (1979) 25

Katz v. United States,
389 U.S. 347 (1967) 2, 8, 11, 12-13

Kyllo v. United States,
533 U.S. 27 (2001) 20-21, 24,26

Los Angeles v. Patel,
135 S. Ct. 2443 (2015) 17

Lucas v. South Carolina Coastal Council,
505 U.S. 1003 (1992) 25

Nollan v. California Coastal Comm'n,
483 U.S. 825 (1987) 25

Olmstead v. United States,
277 U.S. 438 (1928) 8, 10-11

Peterson v. Idaho First Nat'l Bank,
367 P.2d 284 (Idaho 1961) 29

Riley v. California,
134 S. Ct. 2473 (2014) 6-7, 22

Smith v. Maryland,
442 U.S. 735 (1979) 14

South Dakota v. Opperman,
428 U.S. 364 (1976) 6

Terry v. Ohio,
392 U.S. 1 (1968) 5-6

U.S. Trust Co. v. New Jersey,
431 U.S. 1 (1977) 29

United States v. Ackerman,
831 F. 3d 1292 (6th Cir. 2016) 22-23

United States v. Jacobsen,
466 U.S. 109 (1984) 15

United States v. Jones,
132 S. Ct. 945 (2012) 18, 19, 22, 24

United States v. Miller,
425 U.S. 435 (1976) 17

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 22

Statutes

12 U.S.C. § 1829b(a)(2) (2000) 16

18 U.S.C. § 2703(d) 20, 25, 31

The Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 12 U.S.C. §§ 1951–59. (2000)) 16

Other Authorities

Black's Law Dictionary (6th ed. 1990) 26

Federal Trade Comm'n, "Enforcing Privacy Promises" webpage, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises 29

Gerald W. Brock, *The Second Information Revolution* (2003) 10

Jim Harper, *Administering the Fourth Amendment in the Digital Age*, Nat'l Const. Center 19

Jim Harper, *Escaping Fourth Amendment Doctrine After Jones: Physics, Law, and Privacy Protection*, 2011–2012 Cato Sup. Ct. Rev. 219 (2012) 9-10

Mark Taticchi, *Note: Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures*, 78 Geo. Wash. L. Rev. 476 (2010) 20

MetroPCS Privacy Policy, https://www.metropcs.com/terms-conditions/privacy.html 28

MetroPCS Terms & Conditions, https://www.metropcs.com/terms-conditions/terms-conditions-service.html 28

Orin Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. Chi. L. Rev. 113 (2015) 13

Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 ... 11, 21, 26-27

Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85 (2014) 24

T-Mobile Privacy Policy, December 4, 2010 snapshot, http://bit.ly/2vQ64DQ 28-29, 30-31

T-Mobile Terms & Conditions, December 7, 2010 snapshot, http://bit.ly/2wJi6ev 28

Tony Honoré, *Ownership*, in Oxford Essays on Jurisprudence (A.G. Guest ed., 1961) 25

Noah Webster, An American Dictionary of the English Language (1828) 23, 26

2 William Blackstone, Commentaries 25

INTEREST OF *AMICI CURIAE*[1]

Founded in 1984, the **Competitive Enterprise Institute** ("CEI") is a non-profit public policy organization dedicated to advancing the principles of limited government, free enterprise, and individual liberty. CEI frequently publishes research and commentary on topics at the intersection of property rights, markets, free enterprise, and liberty. The instant case concerns CEI because proper administration of the Fourth Amendment would allow businesses to protect their customers' privacy consistent with their interests as determined in the marketplace.

The **Cato Institute** was established in 1977 as a nonpartisan public policy research foundation dedicated to advancing the principles of individual liberty, free markets, and limited government. Cato's Center for Constitutional Studies promotes the principles of limited constitutional government that are the foundation of liberty. To those ends, Cato publishes books and studies, conducts conferences, produces the annual *Cato Supreme Court Review*, and files *amicus* briefs. The present case centrally concerns Cato because it represents an opportunity to improve Fourth Amendment doctrine and maintain that provision's protections in the modern era.

Reason Foundation is a nonpartisan and nonprofit public policy think tank founded in 1978. Reason's mission is to advance a free society by developing, applying, and promoting libertarian principles and policies –including free markets, individual liberty,

---

[1] All parties lodged blanket consents with the Clerk. No counsel for any party authored this brief in whole or in part and no person or entity other than *amici* funded its preparation or submission.

and the rule of law. Reason supports dynamic market-based public policies that allow and encourage individuals and voluntary institutions to flourish. Reason advances its mission by publishing Reason magazine, as well as commentary on its websites, www.reason.com, reason.org, and www.reason.tv. To further Reason's commitment to "Free Minds and Free Markets," Reason selectively participates as *amicus curiae* in cases raising significant constitutional issues.

Founded in 2002, the **Committee for Justice** (CFJ) is a nonprofit, nonpartisan organization dedicated to promoting the rule of law, including the Constitution's limits on the power of government and its protections of individual liberty, including the Fourth Amendment right to be free from unreasonable searches and seizures. CFJ is particularly concerned with the threat to these protections posed by a misfit between existing law—in this case, the "reasonable expectation of privacy" test and the third-party doctrine—and rapid technological advances.

INTRODUCTION AND SUMMARY OF ARGUMENT

For nearly 40 years,[2] this Court and courts below have struggled with using a sociological method for interpreting the Fourth Amendment in difficult cases. They have asked whether government agents disturbed a "reasonable expectation of privacy," reasoning backward from the answer to whether or not a "search" offensive to the Constitution has occurred.

That methodology has been difficult for courts to apply consistently, and in recent years this Court has

---

[2] *Katz v. United States*, 389 U.S. 347 (1967), was decided on December 18, 1967.

used it less and less often as a decision rule. This Court should shed that sociological approach and adopt a juridical method for applying the Fourth Amendment. It should assess the facts of the case in terms of the law, encouraging lower courts to do the same.

Specifically, the Court should examine the following questions:

- Was there a search?
- Was there a seizure?
- Was any search or seizure of "persons, houses, papers, [or] effects"?
- Was any such search or seizure reasonable?

Using that simple and familiar legal methodology would allow this Court to address directly the challenging questions this case presents, including: When does a seizure of data occur? When does a search of data occur? When is data a constitutional "paper" or "effect"? Who has property rights in data sufficient to assert Fourth Amendment rights in it?

The government's compulsory acquisition of data in this case was a seizure. Processing the data to make it human-readable was a search. The records were in relevant part the property of Messrs. Carpenter and Sanders, who enjoyed contractual rights and regulatory protections making them so. And digital documents are best treated as constitutional "papers" or "effects."

That leaves the question whether it was reasonable for the government to seize and search them. There is a presumption in favor of the warrant requirement suggested by the text of the Fourth Amendment, and it is confirmed by this Court's precedents. Thus, it was

unreasonable to seize and search the data without a warrant. Lacking exigency or other excuse, the government should have gotten one.

The interests of Messrs. Carpenter and Sanders are not paramount to *amici*, of course. But as the importance of digital communications and data grows in society, the imperative to straightforwardly address their legal and constitutional status rises.

Without breaking from precedents, this Court can revise Fourth Amendment practice and determine when and how communications and data fit into the Fourth Amendment's categories of protected things. Doing so would permit courts below to address seizures and searches of communications and data forthrightly, confidently assessing the reasonableness of such government action. Here, the result of that analysis calls for the Court to find in favor of the petitioner.

ARGUMENT

I. THIS COURT SHOULD APPLY THE TERMS OF THE FOURTH AMENDMENT IN ALL FOURTH AMENDMENT CASES

The first phrase of the Fourth Amendment says, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const., amend. IV. Absent confusing doctrine, courts would analyze its elements as follows:

- Was there a search?
- Was there a seizure?
- Was any search or seizure of "persons, houses, papers, [or] effects"?

- Was any such search or seizure reasonable?

If there was a search or seizure, if it was of protected things, and if it was unreasonable, then the right has been violated. That is how to administer the Fourth Amendment.

In cases dealing with familiar objects, this Court applies the Fourth Amendment consistent with the language of the law. It looks for seizures and searches of defendants' protected items, then assesses whether or not they were reasonable. (Seizures often precede searches, so reversing the order in which the Fourth Amendment lists them is sensible.)

In *Terry v. Ohio*, 392 U.S. 1 (1968), for example, this Court applied the Fourth Amendment soundly, creating a lasting and useful precedent. The government had urged the Court to place brief "stop and frisk" incidents like a pat-down outside the scope of the Fourth Amendment, *id.* at 16 n.12., arguing that police behavior short of a "technical arrest" or a "full blown-search" did not implicate constitutional scrutiny. *Id.* at 19. This Court rejected the idea that there should be a fuzzy line dividing "stop and frisk" from "search and seizure."

Instead, this Court wrote with granular precision about the seizure, then the search, of Terry: "[T]here can be no question . . . that Officer McFadden 'seized' petitioner and subjected him to a 'search' when he took hold of him and patted down the outer surfaces of his clothing." *Id.* One following the other, the seizure and search were reasonable and therefore constitutional.

Justice Douglas dissented from the ruling but agreed that Terry was "seized" within the meaning of

the Fourth Amendment. *Id.* at 35 (Douglas, J., dissenting). "I also agree," he wrote, "that frisking petitioner and his companions for guns was a 'search.'" *Id.*

Terry and its progeny demonstrated their value again in the recent *Riley v. California* decision, 134 S. Ct. 2473 (2014). Numerous seizures and searches of familiar objects like cars and people were administered using direct application of the Fourth Amendment's terms rather than odd and derived doctrine.

In *Riley*, Officer Charles Dunnigan pulled David Riley over, seizing him and his car consistent with the application of the Fourth Amendment to traffic stops in *Brendlin v. California*. 551 U.S. 249, 254–63 (2007). Upon learning that Riley was driving with a suspended driver's license, Officer Dunnigan removed him from the car, continuing the original seizure of Riley with an additional legal basis for doing so: reasonable suspicion of another violation.

Officer Ruggiero prepared the car for impoundment, a further seizure, consistent with a policy that prevents suspended drivers from returning to, and continuing to operate, their vehicles. He began an "impound inventory search" of the car, as approved in *South Dakota v. Opperman*. 428 U.S. 364, 376 (1976).

That search turned up guns in the engine compartment of the car, so Officer Dunnigan placed Riley under arrest, continuing the ongoing seizure of Riley's body under new legal authority. Officer Dunnigan conducted a search incident to arrest—permitted to aid in the discovery of weapons or of evidence that suspects might destroy. *Chimel v. California*, 395 U.S. 752, 762–63 (1969). Consistent with standard practice for a "booking search," yet another legal basis for both

searching suspects and seizing their property, *see, e.g.*, *Illinois v. Lafayette*, 462 U.S. 640 (1983), Officer Dunnigan examined Riley's person and seized his possessions, including his cell phone.

All these steps were dogs that didn't bark—government actions unchallenged or fully disposed of in courts below. That is because this Court has given law enforcement and courts the legal tools to dispose of them: identify when seizures and searches of protected things have occurred, then determine whether or not they are reasonable.

Courts are well-equipped to make those legal and fact-specific judgments. If the constitutionality of all these investigatory steps turned on sociological questions such as whether government agents had defeated a society-wide "reasonable expectation of privacy," this Court would have a full docket indeed.

Happily, *the Riley* opinion also assessed the search of the phone as the search that it was, without respect to privacy expectations. Having found that the phone was searched in the absence of exigency, this Court laid down the general rule so strongly implied by the second half of the Fourth Amendment: "get a warrant." 134 S. Ct. at 2495.

This case is not *Riley*. It involves both a seizure of data unconnected to a physical effect and a search of that data. A central question is what rights in the data were seized, and whose they were. The status of data as a "paper" or "effect" needs clearing up, too.

But the Court does not need to retreat to doctrine when communications and data are at issue. Data can be seized under the Fourth Amendment just like people and cars. Data can be searched just like homes.

Treating data consistently with physical items would focus courts on the key Fourth Amendment question: whether given seizures or searches are reasonable. Confusing doctrine stands in the way of their doing so.

II. THIS COURT SHOULD ESCHEW THE UNSOUND "REASONABLE EXPECTATION OF PRIVACY" TEST AND OTHER UNHELPFUL DOCTRINES

Relying on doctrine, the decision below begins by noting an alleged constitutional distinction between communications content and routing information. "In Fourth Amendment cases the Supreme Court has long recognized a distinction between the content of a communication and the information necessary to convey it." J.A. 61-2. An uninitiated lawyer or ordinary American would have difficulty understanding what this has to do with constitutional protection for "persons, houses, papers, and effects," which makes no such distinction.

The court below began as it did because this Court has often fallen back on confusing doctrine when applying the Fourth Amendment in hard cases. But this Court can apply the terms of the Fourth Amendment to communications and data cases in a granular way, as it has in the past.

A line of opinions extending from *Ex Parte Jackson*, 96 U.S. 727 (1878), through Justice Butler's dissent in *Olmstead v. United States*, 277 U.S. 438 (1928), and the majority opinion in *Katz v. United States*, 389 U.S. 347 (1967), shows how to integrate communications and data with the Fourth Amendment's textual frame-

work. But a detour over the last forty years into "reasonable expectations" doctrine has undercut sound administration of the Fourth Amendment.

A. *Ex Parte Jackson* Properly Protected Communications in Transit by Protecting Papers and Effects as Such

This Court correctly applied the Fourth Amendment to communications in *Ex Parte Jackson*, 96 U.S. 727 (1878). The opinion did not state in bullet-point order that the postal mail in question, having been handed over to the government, was a) searched, b) a paper or effect, and c) unreasonably searched without a warrant. But it held that "[l]etters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles." *Id.* at 733.

Mailed items remain the papers and effects of their owners while in transit, even though they are not in the possession of their owners. Accessing their contents, such as by opening envelopes, unfolding papers and such, is a search. Doing those things requires a warrant.

The outward form and weight of such items, not being sealed from inspection, are not constitutionally protected. This was early acknowledgement of the difference between what we now call "plain view" and what might be called "plain concealment." It takes no search to discover what is in plain view, so the Fourth Amendment is not implicated. *See Horton v. California*, 496 U.S. 128 (1990). It takes a search to reveal concealed matter, so the Fourth Amendment pertains. The issues are put in play by constitutional text and

disposed of using physics and law, not privacy expectations. *See* Jim Harper, *Escaping Fourth Amendment Doctrine After* Jones*: Physics, Law, and Privacy Protection*, 2011–2012 Cato Sup. Ct. Rev. 219 (2012).

Here, the court below, thrown off by more recent doctrine, treated *Jackson* as a special rule about communications. J.A. 61-6. But *Jackson* simply applied common sense: exposed facts do not require a search to be discovered, even when they are facts about papers and effects. Under *Jackson*, communications written on the outside of an envelope would not be protected, because *Jackson* did not create a content/non-content distinction.

In the year this Court decided *Ex Parte Jackson*, both Western Union and the Bell Company began establishing voice telephone services, Gerald W. Brock, *The Second Information Revolution* 28 (2003). This Court would face that technology after the passage of some time, but perhaps 1928 was too soon because the Court did not soundly address the parallels between postal and telephonic communications in *Olmstead*.

B. *Olmstead* Involved Seizures and Searches of a Wire and Electronic Papers/Effects

Fifty years after *Jackson*, *Olmstead v. United States*, 277 U.S. 438 (1928), incoherently declared wiretapping "the use of the sense of hearing, and that only." *Id.* at 464. A telephone communication renders sounds as electronic signals that travel invisibly and inaudibly along a wire, to be re-formed into audible sounds at the other end. Collecting those signals and reproducing them requires attachments, equipment, and processing well beyond simple hearing.

Justice Butler's dissent stands out because he followed the same sensible lines drawn in *Jackson*, even though the media were now wire and electrons instead of paper and ink. Though he left implicit the physical protections for these communications, Justice Butler identified the private law protections arrayed around telephonic communications. Seizure and search disrupted those arrangements when government agents wiretapped a telephone line: "The contracts between telephone companies and users contemplate the private use of the facilities employed in the service," he wrote. "The communications belong to the parties between whom they pass. During their transmission, the exclusive use of the wire belongs to the persons served by it." *Id.* at 487 (Butler, J., dissenting).

Government agents invaded property rights in the physical wire and in the communication running over it. Specifically, the government's use of the wire and copying of the electronic effects eviscerated Olmstead's right to exclude others from his property—a small but constitutionally significant seizure. The contemporaneous rendering of the communication signal into an audible sound was a search of it. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 551 (2005) ("[A] search occurs when information from or about the data is exposed to possible human observation."). The wiretap should have required a warrant.

It would have taken prescience indeed to recognize in the 1920s that telephonic and later digital communications would be the scions of physical mail. *But see Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting) ("Ways may someday be developed by which the Gov-

ernment, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.") Even now, the idea that papers and effects may take electronic or digital form takes some getting used to. But that ground is long since broken. The Court's treatment of a suitably shrouded oral communication as a constitutionally protected item in *Katz* has been widely accepted.

C. The *Katz* Majority Inarticulately Applied the Fourth Amendment's Terms to a Shrouded Oral Communication

Regrettably, when the Court reversed *Olmstead*, it avoided stating directly that the suitably concealed sound of a person's voice is a transitory "effect." (If the language of the Fourth Amendment applies, it almost certainly must be.) And even more unfortunately, the popular treatment of *Katz v. United States*, 389 U.S. 347 (1967), has been to ignore the majority's reasoning in favor of Justice Harlan's solo concurrence, which attempted to reframe Fourth Amendment jurisprudence around "reasonable expectations of privacy."

But the *Katz* majority decision was an inarticulate parallel to *Ex Parte Jackson*. The Court followed the same line as *Jackson* about disclosed matter requiring no search and concealed things requiring a seizure or search. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351 (citations omitted).

The paragraphs that followed discussed the import of Katz's going into a phone booth made of glass, which concealed the sound of his voice. *Id.* at 352. Against the argument that Katz's body was in public for all to see, the Court wrote: "[W]hat he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear." *Id.* The government's use of a secreted listening and recording device to enhance ordinary perception overcame the physical concealment Katz had given to his voice. Gathering the sound waves seized something of Katz's.

But in his solo concurrence, which was unnecessary to the outcome of the case, Justice Harlan shared his sense of how the Constitution controls government access to private communications: "My understanding," he wrote, "is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.* at 361. Justice Harlan's understanding has not aided courts' administration of Fourth Amendment cases.

D. The Ills of the "Reasonable Expectation of Privacy" Test

Since *Katz*, courts have often followed Justice Harlan's concurrence, attempting to analyze whether defendants have had a "reasonable expectation of privacy" in information or things. Under Harlan's concurrence, but not the *Katz* majority's rationale, the existence and defeat of a "reasonable expectation of privacy" signals a constitutional search generally requiring a warrant.

Alas, courts rarely perform the full analysis. They infrequently inquire into a defendant's "actual (subjective) expectation of privacy," for example, or how it was "exhibited." *See* Orin Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. Chi. L. Rev. 113 (2015).

The second half of the test invites justices and judges to try to assess the entire society's emergent views on privacy. That is a sociological exercise, not a juridical one. It does not involve the application of law to facts or fact-specific judgments. It requires judges to use their own views or best estimations about the privacy interests of the whole society.

A particularly poor example of the test as applied is the opinion in *Smith v. Maryland*, 442 U.S. 735 (1979), in which Justice Blackmun walked through influences that would suppress expectations of privacy in phone-dialing information and none that would support it. *See id.* at 742–43. The court below here relied heavily on *Smith*, which in addition to being poorly reasoned may also be distinguished, given the great quantities of data at stake in cases like the present one.

The subjectivity of Justice Harlan's formulation is compounded by its essential circularity. Societal expectations guide judicial rulings, which guide societal expectations, and so on. That circularity is especially problematic here at the onset of the Information Age because digital communications and data are only beginning to take their place in society. Expectations about privacy in this medium are still taking form, and the technology continues to change, so there is simply no objectively reasonable sense of privacy for judges to discover.

E. Corollaries of the "Reasonable Expectation of Privacy" Test Are Even Worse

The "reasonable expectation of privacy" test has at least two corollaries that move doctrine even further from the Fourth Amendment's language and meaning. The first is the doctrine that treats searches tailored for illegal things as non-searches. The second is the "third-party doctrine," which denies that shared things can be unreasonably seized or searched.

Illinois v. Caballes, 543 U.S. 405 (2005), is typical of "reasonable expectation" cases in that it did not examine (or even assume) whether Roy Caballes had exhibited a subjective expectation of privacy in the trunk of his car when government agents subjected it to the ministrations of a drug-sniffing dog. Thus, the Court could not take the second step, examining its objective reasonableness.

Instead, the *Caballes* Court skipped forward to a corollary of the "reasonable expectations" test that the Court had drawn in *United States v. Jacobsen*, 466 U.S. 109 (1984): "Official conduct that does not 'compromise any legitimate interest in privacy' is not a search subject to the Fourth Amendment." *Caballes*, 543 U.S. at 408 (quoting *Jacobsen*, 466 U.S. at 123). Possession of drugs being illegal, there is no legitimate expectation of privacy in their possession. Thus, a search aimed at illegal drugs is not a search. That's confounding.

That entirely logical extension of "reasonable expectations" doctrine reveals the doctrine's role in delinking Fourth Amendment decisions from the Fourth Amendment's text. Now, instead of examining whether searches and seizures are reasonable, courts

applying the *Jacobsen/Caballes* corollary can uphold any activity of government agents that appears sufficiently tailored to discovering only crime. The most intensive government examination of persons, houses, papers, and effects can be "not a search," *id.*, no matter how intimate it is, no matter how often it recurs, and irrespective of any context or circumstances.

The second corollary of "reasonable expectations" doctrine, more relevant here, similarly breaks the link between the terms of the law and outcomes in cases. That is the "third party doctrine," which the court below relied on here.

The Bank Secrecy Act ("BSA"), Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 12 U.S.C. §§ 1951–59. (2000)) requires banks to maintain records and file reports with the Treasury Department if they "have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings." 12 U.S.C. § 1829b(a)(2) (2000). In *California Bankers Ass'n v. Shultz*, 416 U.S. 21 (1974), several parties challenged the BSA's requirements. The records-collection part of the law does not require disclosure to the government, so the Court found that it does not implicate the Fourth Amendment. *Id.* at 54. As to the reporting requirements, the Court denied standing to bank depositors who could not show that information about their financial transactions had been reported. *Id.* at 67–68.

Justice Thurgood Marshall criticized how the Court avoided finding that mandated record-keeping affects a constitutional seizure just because the government would acquire the records later. "By accepting the Government's bifurcated approach to the recordkeeping requirement and the acquisition of the records, the majority engages in a hollow charade whereby Fourth

Amendment claims are to be labeled premature until such time as they can be deemed too late." *Id.* at 97 (Marshall, J., dissenting).

Two years later, in *United States v. Miller*, 425 U.S. 435 (1976), the Court held that a defendant had no Fourth Amendment interest in records maintained about him pursuant to the BSA. *Id.* at 442–43. It did not examine whether the operation of the BSA was a seizure or search, but used "reasonable expectations" doctrine to dismiss Miller's Fourth Amendment interests in documents reflecting his financial activities. This was because they were held by a financial services provider: "we perceive no legitimate 'expectation of privacy' in their contents." *Id.* at 442.

Under these cases, the government can compel a service provider to maintain records about a customer and then collect those records without implicating his or her Fourth Amendment rights. *Cf. Los Angeles v. Patel*, 135 S. Ct. 2443 (2015) (holding requirement that hotel operators make their guest registries available to the police on demand facially unconstitutional). The rule of *Miller* appears to be that Americans forfeit their Fourth Amendment interests in any material that comes into possession of a third party. This at least elides subtler questions about who owns communications and data such as to enjoy a right to their protection from unreasonable seizure and search.

Based as they are in "reasonable expectations" doctrine, these holdings are hard to square with the Fourth Amendment's text. And they grow further out of synch with each step forward in modern, electronically connected living.

Incredibly deep reservoirs of information are constantly collected by third-party service providers today. Cellular telephone networks pinpoint customers' locations throughout the day through the movement of their phones. Internet service providers maintain copies of huge swaths of the information that crosses their networks tied to customer identifiers. Search engines maintain logs of searches that can be correlated to specific computers and the individuals that use them. Payment systems record each instance of commerce and the time and place it occurred. This trend will only accelerate as the "Internet of Things" supplies data revealing more and more of our activities—even use of our household appliances—to third-party service providers.

The totality of these records are very, very revealing of innocent people's lives. They are a window onto each individual's spirituality or religion, feelings, and intellect. They can reveal excruciatingly intimate details about physical and mental health, as well as marital and family relations. They reflect each American's beliefs, thoughts, emotions, sensations, and relationships. Their security ought to be protected from unreasonable seizure—as they are the modern iteration of our papers and effects. *See United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). These items should generally not be seized without a warrant.

Thanks to recent cases, this Court is positioned to apply traditional common-law concepts such as property rights to digital communications and data, placing them within the framework set out by the text of the Fourth Amendment.

III. THIS COURT'S RECENT CASES ARE A FRAMEWORK FOR ADMINISTERING THE FOURTH AMENDMENT IN A RELIABLE AND JURIDICAL WAY

Familiar but circular and misleading doctrine like the "reasonable expectation of privacy" test does not square the Fourth Amendment's terms with the facts in particular cases. This Court's recent Fourth Amendment opinions, though, provide a framework for a clear return to adjudicating the Fourth Amendment as a law, even in difficult "high-tech" cases. *See* Jim Harper, *Administering the Fourth Amendment in the Digital Age*, Nat'l Const. Center, https://constitutioncenter.org/digital-privacy/The-Fourth-Amendment-in-the-Digital-Age. In all cases, the Court can follow the methodology suggested by the Fourth Amendment, which is to look for searches, look for seizures, determine whether they go to constitutionally protected items, and then determine whether they are reasonable.

This does not mean that the precise way to apply the Fourth Amendment's terms to communications and data is already obvious. It requires this Court to integrate advancing technology with long-standing legal principles. In doing so, this Court should find that data and digital communications are property that can be seized and searched even when the owners of the data are not in possession of it.

A. *Jones* Was a Seizure Case

Though this Court referred to what happened in *United States v. Jones*, 132 S. Ct. 945 (2012), as a "search," the precipitating constitutional invasion was a seizure. That seizure occurred when government agents attached a device to a car that was not theirs,

making use of it to transport their device without a warrant. *Id.* at 949; *see ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (referring to attachment of GPS device in *Jones* as "a technical trespass on the defendant's vehicle"). Though small, that seizure of Jones's car was real. It abrogated Jones's right to exclude and awarded the government a right to use the vehicle for its purposes. That was a sufficient trigger of scrutiny for constitutional reasonableness. The seizure facilitated a weeks-long, contemporaneous search for Jones's location. Considering the outsized effect on Jones, who was still presumed innocent, the seizure and the search were unreasonable without a warrant.

The present case is a much simpler seizure case. The government here seized data under authority given by 18 U.S.C. § 2703(d). J.A. 61-3. When government agents copy data or information that is otherwise unavailable to them, they have taken the rights to use and enjoy that data's benefits for the government, and the owner's right to exclude others has been eviscerated. *See* Mark Taticchi, *Note: Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures*, 78 Geo. Wash. L. Rev. 476, 491–96 (2010). From the beginning of its analysis, this Court should recognize data as something that can be seized.

Is it a "paper" or "effect"? Is it the defendant's paper or effect in which to assert a right? These questions come later in a methodical analysis.

B. *Kyllo* Is a High-Tech Search Case

Though less relevant here, this Court's opinion in *Kyllo v. United States*, 533 U.S. 27 (2001), is a wonder-

fully instructive modern "search" case, because it features a search in the absence of seizure. That allows us to observe search in the abstract and see how concealment subjected to search produces exposure. Bringing exposure to concealed things is a strong signal that a search has occurred.

The thermal-imaging camera used to incriminate the petitioner in *Kyllo* detected radiation in the infrared range of the electromagnetic spectrum (that is, radiation with longer wavelengths than visible light). It produced an image of that radiation called a thermogram by representing otherwise invisible radiation in the visible spectrum. That made imperceptible radiation perceptible to humans.

Using a thermal imager on a house was a search of its exterior for information about what transpired inside, and the Court found it so. "Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion," the Court held, "the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Kyllo*, 533 U.S. at 40. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 553 (2005) ("For the holding in *Kyllo* to make sense, it must be the transformation of the existing signal into a form that communicates information to a person that constitutes the search. What made the conduct in *Kyllo* a search was not the existence of the radiation signal in the air, but the output of the thermal image machine and what it exposed to human observation.").

C. "Papers" and "Effects" Can Take a Digital Form

This Court has often been relatively clear that searched or seized items are within the categories listed for protection in the Fourth Amendment. In other cases, it is an essential inference of the Court's rulings. But the best practice would be to consistently and systematically recite each element of the Fourth Amendment as a model for lower courts.

The categorization of digital materials as paper, effects, or otherwise, as well as the ownership status of such items, are questions that would benefit from sharpening by this Court in this case. Significantly, the *Jones* Court declared the existence of a constitutionally protected item: "It is beyond dispute that a vehicle is an 'effect' as that term is used in the Amendment." 132 S. Ct. at 949. And it detailed the property question, finding that Jones "had at least the property rights of a bailee." *Id.* at 949 n.2. The possessive pronoun in the Fourth Amendment circumscribes the items in which defendants may assert Fourth Amendment interests.

Riley, of course, dealt with the unconstitutional search of a cell phone. By necessary inference, phones themselves are effects.

Dictum in *Riley* suggests that digital files in phones are effects, too. In declining to allow warrantless cellphone searches of a phone that may contain evidence of the crime of arrest, 134 S. Ct. at 2492, the *Riley* Court said that doing so would "in effect give police officers unbridled discretion to rummage at will among a person's private effects." *Id.* (quotation and citation omitted). This Court treated not just phones, but the

documents and materials they hold, as effects. It did not matter that they were digital.

Seven years ago, the Sixth Circuit found constitutional protection for email, which also must rest on the premise that digital data in the form of an email file is a "paper" or "effect" for Fourth Amendment purposes. In *United States v. Warshak*, that court said: "Given the fundamental similarities between email and traditional forms of communications, it would defy common sense to afford emails lesser Fourth Amendment protection. Email is the technological scion of tangible mail." 631 F.3d 266, 285–86 (6th Cir. 2010).

And last year the Tenth Circuit explicitly treated an email with attachments as "a 'paper' or 'effect' for Fourth Amendment purposes." None of the litigants had disputed that essential premise. *United States v. Ackerman*, 831 F. 3d 1292, 1304 (6th Cir. 2016).

The word "papers," of course, should not be taken narrowly as a "substance formed into thin sheets on which letters and figures are written or printed," but rather as "|a|ny written instrument, whether note, receipt, bill, invoice, bond, memorial, deed, and the like." N. Webster, *An American Dictionary of the English Language* (1828). The broad sense of the term is consistent with deep precedent. *Boyd v. United States*, 116 U.S. 616 (1886), for example, speaks numerous times of "books and papers" and "books, invoices, and papers." *Id.* at *passim*. Taking "papers" too narrowly would have Justice Bradley repeating himself incoherently: Books at the time were made largely of paper, invoices were made of paper, and papers were also, of course, made of paper. "Papers" was the broad cate-

gory of instruments on or in which people collect information to the *Boyd* Court, and to the Framers of the Fourth Amendment.

The parallel between email and tangible mail is the beginning but not the end of the relationship between digital files and the "papers" and "effects" categories. Again, the Fourth Amendment does not have special rules for communications, but covers all papers and effects equally. Email is but one of many protocols that replicate and expand on people's ability to collect, store, and transmit personal information as they did in the founding era. This court would best treat digital files as papers or effects, regardless of its determinations about their ownership status and the reasonableness of seizing and searching particular files in any given case. The coverage of the Fourth Amendment must extend to these media if this Court is to succeed in "assuring preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34; *United States v. Jones*, 565 U.S. at 950; *id.* at 958 (Alito, J., concurring).

The final question before assessing the reasonableness of government action is whether a constitutionally protected item is the defendant's. Just as with telephones according to Justice Butler's view in *Olmstead*, people use modern communications and Internet facilities under contracts that allocate property rights. Though hardly with perfect clarity, these contracts detail how communications machinery will be used, and they divide up the ownership of information and data. *See* Scott R. Peppet, *Regulating the Internet*

of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 Tex. L. Rev. 85, 142–45 (2014).

The court below, applying doctrine, back-handedly dismissed this crucial question: whether the defendants had a property right in the data that the government seized. J.A. 61-8 ("The defendants of course lack any property interest in cell-site records."). This Court should clarify the importance of property principles for administering the Fourth Amendment—it lists items of property, after all—reversing the court below and modeling for future courts how this is done with care.

IV. THE GOVERNMENT SEIZED AND SEARCHED PETITIONER'S DIGITAL PAPERS, WHICH WAS UNREASONABLE WITHOUT A WARRANT

Applying the terms of the Fourth Amendment to the instant case shows that the government seized and searched digital papers in which the petitioner had a relevant ownership interest. Given the requirement for a warrant in all but narrow, exceptional cases, doing so was unreasonable and thus violated their Fourth Amendment rights.

A. There Was a Seizure

The government's invocation of the authority of 18 U.S.C. § 2703(d) to command the disclosure of data was a seizure of that data. The Court should treat it as such because it deprived the owner of a salient property interest, the right to exclude.

This Court has emphasized the "right to exclude others" as "one of the most essential sticks in the bun-

dle of rights that are commonly characterized as property." *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979); *see also Dolan v. City of Tigard*, 512 U.S. 374, 384 (1994); *Lucas v. South Carolina Coastal Council*, 505 U.S. 1003, 1044 (1992); *Nollan v. California Coastal Comm'n*, 483 U.S. 825, 831 (1987). Blackstone's definition of property also featured the right to exclude: "[property is] that sole and despotic dominion which one . . . claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe." 2 William Blackstone, Commentaries *2.

There is an argument that data is not seized when its original owner still has a copy. But that argument is unavailing because it treats possession as the only important property right. It is not. The right to possess property is only one of several aspects of ownership identified in legal philosophy. *See generally* Tony Honoré, *Ownership*, in Oxford Essays on Jurisprudence 104-147 (A.G. Guest ed., 1961).

B. There Was a Search

Given the existence of a constitutional seizure of the data, a search of it need not be established to proceed to further steps in the Fourth Amendment analysis. But searches of data will be a relevant issue before this Court and others in the future, so it is at least an important detail.

By causing computers to render it in human-readable form, government agents searched the data they had seized in order to learn the whereabouts of Carpenter and Sanders during the relevant time-periods.

Putting aside confusing doctrine in favor of natural language, "'Search' consists of looking for or seeking

out that which is otherwise concealed from view." *Black's Law Dictionary* 1349 (6th ed. 1990). In *Kyllo*, this Court said, "When the Fourth Amendment was adopted, as now, to 'search' meant '[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book; to *search* the wood for a thief.'" *Kyllo*, 533 U.S. at 32 n.1, quoting N. Webster, *An American Dictionary of the English Language* 66 (1828) (reprint 6th ed. 1989).

Communications and data, just like other things, can be looked through with the purpose of finding something. They are searched when their contents are converted in format, bringing information out of concealment into exposure.

In his article, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005), Professor Orin Kerr intricately analyzes the technical details of computer processing as it relates to government investigations. *Id.* at 549-51. "The best answer," he concludes, "is that a search occurs when information from or about the data is exposed to possible human observation." *Id.* at 551. Here, the government's agents did that with the data they had earlier seized.

C. "Papers" or "Effects" Were Involved

Putting aside for the moment whose it was, there is little basis for arguing that the data seized are not constitutional papers or effects. As discussed above, the relevant meaning of "papers" in the Fourth Amendment is not thin sheets of ink-absorbent material but any corpus or collection of information.

The court below referred to the data in question as "business records" several times. This would tend to

confirm that they are collections of information qualifying as constitutional papers. That usage elided the distinct question of whose records they are, however.

D. Carpenter and Sanders Owned Them

The Fourth Amendment uses the possessive pronoun "their" to modify "persons, houses, papers, and effects." Doing so limits who can claim the protections of that law with respect to any such item. In relevant part, the data that the government seized was the property of Messrs. Carpenter and Sanders. It was not the property of their cellular providers, MetroPCS and T-Mobile, to give to the government.

In this area, again, careful attendance to property concepts helps draw the lines. They may be "business records"—information collected by a business for business purposes—but that does not make them automatically the property *in toto* of the business.

Consumer-facing digital businesses, including telecommunications providers, enter into very detailed arrangements that divide up ownership of information about customer use of their services. Communications providers are also subject to regulations that similarly allocate rights to exclude, use, sell, and process information.

When people use digital and communications services, they share and produce personal information that can be sensitive, intimate, and privileged. This is why the T-Mobile and MetroPCS user agreements and privacy policies allocate the bulk of rights to control and use personal data to customers, consistent with practice across digital services. These property rights in data include the right of users to exclude others

from personal data in all but closely defined circumstances.

The T-Mobile privacy policy in effect in late 2010,[3] which was incorporated by reference into the company's terms of service, *see* T-Mobile Terms & Conditions, December 7, 2010 snapshot, http://bit.ly/2wJi6ev, is typical in that it denies T-Mobile rights to sell or share data except as provided in the policy. "We do not sell, rent, or otherwise provide your personal information to unaffiliated third-parties (parties outside the T-Mobile corporate family) to market their services or products to you. We may, however, disclose your personal information to unaffiliated third-parties as follows:" T-Mobile Privacy Policy, December 4, 2010 snapshot, http://bit.ly/2vQ64DQ [hereinafter "2010 T-Mobile Contract"]. This leaves the general right to exclude all others from the data with the customer. The possessive pronoun "your" signifies that the bulk of the ownership of the data is the customer's.

Contract terms limiting access to personal information have a long history. *See, e.g., Peterson v. Idaho First Nat'l Bank*, 367 P.2d 284, 290 (Idaho 1961), *quoting* 7 Am.Jur., Banks, § 196 ("[I]t is an implied term of the contract between a banker and his customer that the banker will not divulge to third persons, without the consent of the customer, express or implied, either

---

[3] The current MetroPCS Terms and Conditions and privacy policy are similar in all material ways to T-Mobile's commitments, though the precise language varies. *See* https://www.metropcs.com/terms-conditions/terms-conditions-service.html and https://www.metropcs.com/terms-conditions/privacy.html. Probably due to a change in the URL structure of the MetroPCS site, versions of these documents contemporaneous to the events in this case could not be found.

the state of the customer's account or any of his transactions with the bank, or any information relating to the customer acquired through the keeping of his account, unless the banker is compelled to do so by order of a court, [or] the circumstances give rise to a public duty of disclosure").

In the modern era, much enforcement of these rights is by government agencies standing in for consumers. *See, e.g.*, Federal Trade Comm'n, "Enforcing Privacy Promises" webpage, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises. But there is also active litigation that asserts violation of contracts pertaining to terms of service, privacy policies, and the like. *See, e.g., In re Facebook Internet Tracking Litigation*, No. 5:12-md-02314-EJD (N.D. Cal. filed Feb. 8, 2012). These rights are property rights. *See U.S. Trust Co. v. New Jersey*, 431 U.S. 1, 19 n.16 (1977) ("Contract rights are a form of property"). There is no juridical way to characterize the exchange of promises between T-Mobile and its customers other than as contracts allocating property rights.

The exceptions to the general rule, allocating certain rights to T-Mobile, are also typical of privacy policies. T-Mobile may share personal information with service providers and merger partners subject to relevant constraints. The contract allows T-Mobile to share information with other third parties "with your consent," 2010 T-Mobile Contract. By inference, the right to sell, like the bulk of the rights to the data, rests with the customer.

One of the exceptions—also typical and appropriate—is the exception for sharing with government and law enforcement. That provision states in relevant

part: "We may disclose personal information or communications where we believe in good faith such disclosure is necessary to comply with the law or respond to legal process (for example, lawful subpoena, court order, E-9-1-1 information)." 2010 T-Mobile Contract.

This provision does not give T-Mobile free rein to hand data over to the government when asked. T-Mobile can only do so when its good faith assessment is that it must comply with law or respond to legal process. T-Mobile may not hand over information when the law does not require it, or when it is faced with something other than "legal process."

At least two senses of that word "legal" are relevant. One is that the procedures are recognized and systematically used procedures in law enforcement and courts. The other is that the procedures comport with the standards laid out in the law.

The contract does not permit T-Mobile to comply with court orders simply because they take a certain form. Such orders must also satisfy the substantive legal merits for divesting a private party of control over the things demanded by the government. T-Mobile only has the right to share the data if the process used to divest the customer of control is both legal in form and substance. To the extent T-Mobile does not resist an invalid or overbroad subpoena, the data is not T-Mobile's to turn over. The data remains the property of the customer.

There is an argument that the T-Mobile privacy policy denies customers the right to exclude others from data that is disclosed pursuant to § 2703(d) because it is a legal process, established by Congress no less. But that begs the question whether the process is

valid and legal. The customer should be able to argue his or her side of that question. Presuming the opposite would make surplus language of important words in the sentence giving T-Mobile only a limited right to provide information to the government.

A customer who is suspected of criminal activity cannot sensibly be invited to participate in adjudicating his or her rights during the investigation, of course. The next step in the analysis makes clear that the solution is to enlist a neutral arbiter.

E. The Government's Actions Were Unreasonable

The final step in the analysis is determining whether it was unreasonable for government agents to seize and search data which in relevant part was Carpenter's and Sanders's to exclude from all others. It was indeed unreasonable.

The structure of the Fourth Amendment suggests, and the Supreme Court's precedents make clear, that getting a warrant is the reasonable thing to do when it can be done. "It is a cardinal rule that . . . law enforcement . . . use search warrants wherever reasonably practicable." *Chimel v. California*, 395 U.S. 752 (1969).

Cell-site location information sits in long-term storage with stable, identified service providers. There is no exigency that threatens its destruction. Imposing the warrant requirement does put a small paperwork burden on law enforcement, but it does so to provide all telecommunications users the benefit of having a check on governmental processes that might otherwise upset the contract-based property rights that undergird their digital privacy protection.

* * *

The analytical framework suggested and used above shows that the government seized and then searched data—constitutional papers—in which Timothy Ivory Carpenter and Timothy Michael Sanders had a relevant property interest. Doing so without a warrant was unreasonable, and thus it violated their constitutional rights. That conclusion hardly forecloses the use of cell site location information in criminal investigations. It merely imposes the procedural check against abuse of having a neutral arbiter sign off on a warrant.

There are cases where cell site location information might be very useful even though neither exigency nor probable cause exist, such as when the data could reveal where a homicide victim was located immediately prior to death. But such situations can be and are accounted for in the contracts that allocate rights to customer data. The T-Mobile contract, for example, allows disclosure in emergency situations and to the primary account holder. For the narrow cases that remain, the terms of such policies could make clear that rights to exclude others from data expire with the customer or are the property of his or her next of kin.

If this Court declines to abandon the sociological approach to Fourth Amendment administration found in the "reasonable expectation of privacy" test, an alternative to merely guessing at what people expect is to consult the very documents that record and define their expectations: the contracts between communications providers and their customers.

People expect privacy in data about their communications because they have contract-based and other property rights to exclude others from it. Reasoning through the elements of the Fourth Amendment in

light of those arrangements is a better model of jurisprudence than guesswork about privacy expectations.

CONCLUSION

Applying the text of the Fourth Amendment to this case, the Court should reverse the decision below.

Respectfully submitted,

Ilya Shapiro
CATO INSTITUTE
1000 Mass. Ave. N.W.
Washington, D.C. 20001
(202) 842-0200
ishapiro@cato.org

Manuel S. Klausner
LAW OFFICES OF MANUEL S. KLAUSNER
One Bunker Hill Building
601 W. Fifth St., Suite 800
Los Angeles, CA 90071
(213) 617-0414
mklausner@klausnerlaw.us

Jim Harper
Counsel of Record
Ryan C. Radia
COMPETITIVE ENTERPRISE INSTITUTE
1310 L St. NW, 7th Floor
Washington, D.C. 20005
(202) 331-1010
jim.harper@cei.org

Curt Levey
The Committee for Justice
722 12th St. NW, 4th Floor
Washington, DC 20005
(202) 270-7748
clevey@committeeforjustice.org

August 11, 2017

RECORD AND BRIEFS

Supreme Court, U.S.
FILED
AUG 11 2017
OFFICE OF THE CLERK

No. 16-402

IN THE
Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

BRIEF OF AMICI CURIAE DATA & SOCIETY RESEARCH INSTITUTE AND FIFTEEN SCHOLARS OF TECHNOLOGY AND SOCIETY IN SUPPORT OF PETITIONER

MARCIA HOFMANN
KENDRA ALBERT
ZEITGEIST LAW PC
25 Taylor St.
San Francisco, CA 94102

ANDREW D. SELBST
Counsel of Record
DATA & SOCIETY
RESEARCH INSTITUTE
36 W. 20th St., 11th Floor
New York, NY 10011
(617) 504-1982
andrew@datasociety.net

Attorneys for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

INTEREST OF *AMICI CURIAE* 1

SUMMARY OF ARGUMENT 4

ARGUMENT 5

I. THE THIRD-PARTY DOCTRINE SHOULD NOT APPLY TO CELL SITE LOCATION INFORMATION BECAUSE CELL PHONE USE IS NOT TRULY VOLUNTARY IN MODERN-DAY SOCIETY. 6

A. The Court Should Adapt the Third-Party Doctrine for the Digital Age by Giving More Substance to the Voluntary Conveyance Requirement. 7

B. The Third-Party Doctrine's Foundational Cases Predating *Miller* and *Smith* Support a More Robust Notion of Voluntary Conveyance. 9

C. The Fourth Amendment's Content/Non-Content Distinction Does Not Solve the Third-Party Doctrine's Problems. 11

II. THE USE OF CELL PHONES IN THE MODERN WORLD IS NOT MEANINGFULLY VOLUNTARY. 14

A. Cell Phones Are Necessary to Participate in the Most Basic Aspects of Everyday Social and Family Life. 14

B. Cell Phones Are Essential Public Safety Infrastructure and Personal Safety Equipment. 17

C. Cell Phones Are Both Necessary to Find Employment and an Important Part of Workplace Infrastructure. 21

D. Cell Phones Are Widely Used for Commerce and Banking and Are Rapidly Becoming Integral. 25

E. Cell Phones Have Become a Key Technology for Civic Participation. 28

F. Cell Phones Are Enabling Better Health Outcomes. 31

G. Cell Phones Are Especially Critical to Vulnerable Populations. 34

H. United States Government Programs and Initiatives Have Recognized the Necessity of Mobile Technology 36

CONCLUSION 39

TABLE OF AUTHORITIES

Cases

City of Ontario v. *Quon*, 560 U.S. 746 (2010) 9

Hoffa v. *United States*, 385 U.S. 293 (1966) 10

Katz v. *United States*, 389 U.S. 347 (1967).....8

Kyllo v. *United States*, 533 U.S. 27 (2001).....5, 8

Lopez v. *United States*, 373 U.S. 427 (1963).....10

Riley v. *California*, 134 S. Ct. 2473 (2014) ...5, 7, 9, 12

Smith v. *Maryland*, 442 U.S. 735 (1979) 5, 8, 11, 12

United States v. *Carpenter*, 819 F.3d 880 (6th Cir. 2016) 11

United States v. *Jones*, 565 U.S. 400 (2012) 5, 7, 11, 12

United States v. *Miller*, 425 U.S. 435 (1976) ....passim

United States v. *White*, 401 U.S. 745 (1971).....10

Other Authorities

Aaron Smith, Pew Research Center, *Labor Platforms: Technology-Enabled 'Gig Work'* (2016) 25

Aaron Smith, Pew Research Center, *Searching for Work in the Digital Era* 2 (2015).....21, 22, 35

Aaron Smith, Pew Research Center, *U.S. Smartphone Use in 2015* (2015) 15, 19

Alessandra Ram, *It's Your Right to Film the Police. These Apps Can Help*, Wired (May 3, 2015) 21

Amanda Lenhart, et al., Pew Research Center, *Teens, Technology, and Friendships* (2015) 17

American Bankers Association, *Survey: More Americans Using Mobile Deposit* (2015).....28

American Red Cross, *Social Media Grows Up – Red Cross Emergency Social Data Summit* (Aug. 12, 2010).....18, 19

Amy L. Gonzales, *Health Benefits and Barriers to Cell Phone Use in Low-Income Urban U.S. Neighborhoods: Indications of Technology Maintenance*, 2 Mobile Media & Comm. 233 (2014).....32, 37

Amy L. Gonzales, Lindsay Ems & Venkata Ratnadeep Suri, *Cell Phone Disconnection Disrupts Access to Healthcare and Health Resources: A Technology Maintenance Perspective*, 18 New Media & Soc'y 1422 (2016).....33, 37

Bill Siwicki, *American Well Partners With Samsung Electronics For Mobile Telehealth*, Healthcare IT News (Feb 21, 2017).....33

Brian Barrett, *Your Phone Will Replace Your Wallet at the ATM, Too*, Wired (Jan. 28, 2016).....26

Brief for Electronic Frontier Foundation, et al. as *Amici Curiae* in Support of Certiorari.....8

Brief in Opposition to Certiorari.....6

Christian Licoppe, *'Connected' Presence: The Emergence of a New Repertoire for Managing Social Relationships in a Changing Communication Technoscape*, 22 Env. & Planning D: Soc'y & Space 135, (2004).....16

City of Boston Apps, City of Boston.....32

College Parents of America, *Survey of Current College Parent Experiences* (2006).....17

ComScore, *The 2016 U.S. Mobile App Report* (2017) 28

D. Keith McInnes, et al., *Retaining Homeless Veterans in Outpatient Care: A Pilot Study of Mobile Phone Text Message Appointment Reminders*, 104 Am. J. Pub. Health S588 (2014) .34

Daniel Greene & Ifeoma Ajunwa, *Automated Hiring Platforms as Technological Intermediaries and Brokers* (work in progress) 22

Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083 (2002) 6

Daniel Schneider & Kristen Harknett, *Schedule Instability and Unpredictability and Worker and Family Health and Wellbeing* (2016) (working paper) 24

Devindra Hardawar, *Google Wallet to Come Pre-Installed on Phones for Major Carriers*, Engadget (Feb. 23, 2015) 26

Dina Bass, *New App Helps Shift Workers Swap Hours*, Boston Globe (July 13, 2016) 24

Emil Protalinski, *Facebook Passes 1.65 Billion Monthly Active Users, 54% Access the Service Only on Mobile*, VentureBeat (Apr. 27, 2016) 19

Encyclopedia of Social Media and Politics (Kerric Harvey, ed. 2014) 31

Eric Tsetsi & Stephen A. Rains, *Smartphone Internet Access and Use: Extending the Digital Divide and Usage Gap*, 5 Mobile Media & Comm. __ (2017) ..35

FDIC, *2015 FDIC National Survey of Unbanked and Underbanked Households* 28, 36

Federal Reserve Board, *Consumers and Mobile Financial Services 2015* (2015) 26

Gerald G. Ashdown, *The Fourth Amendment and the 'Legitimate Expectation of Privacy,'* 34 Vand. L. Rev. 1289 (1981).....6

Gerard Goggin & Christopher Newell, *Disabling Cell Phones*, The Cell Phone Reader: Essays in Social Transformation 155 (2007).....36

Holly Maluk, Myrna Pérez & Lucy Zhou, Brennan Center for Justice, *Voter Registration in a Digital Age: 2015 Update* (2015).....30

Jen Tolentino, Voting Information Project, *VIP Offers Free iOS App* (June 24, 2014).....31

Jim Harter et al., *Most U.S. Workers See Upside to Staying Connected to Work*, Gallup (Apr. 30, 2014) 23

Jonathan Hall & Alan Krueger, *An Analysis of the Labor Market for Uber's Driver-Partners in the United States* (2015) 25

Judy Wajcman, Michael Bittman & Judith Brown, *Families without Borders: Mobile Phones, Connectedness and Work-Home Divisions*, 42 Sociology 635 (2008).....17

Judy Wajcman, Pressed for Time: The Acceleration of Life in Digital Capitalism (2014) 16

Julia Ticona, *In 23 States, Lifeline Participation Higher Than Unemployment Insurance* (Aug. 8, 2017) 38

Karen Mossberger, Caroline J. Tolbert & Christopher Anderson, *The Mobile Internet and Digital Citizenship in African-American and Latino*

Communities, 20 Info. Comm. & Soc'y 1587 (2017) 29

Kathleen M. Cumiskey & Kendra Brewster, *Mobile Phones or Pepper Spray? Imagined Mobile Intimacy as a Weapon of Self-Defense for Women*, 12 Feminist Media Stud. 590 (2012).....20

Knight Foundation, *Mobile-First News: How People Use Smartphones to Access Information* 10 (2016) 30

Kristen Purcell & Lee Rainie, Pew Research Center, *Technology's Impact on Workers* (December 30, 2014) 23

Leena Rao, *Venmo Is On Track to Process $20 Billion in Payments Per Year*, Fortune (Oct. 20 2016).....29

Lewis R. Katz, *In Search of A Fourth Amendment for the Twenty-First Century*, 65 Ind. L.J. 549 (1990) .6

Linda K. Moore, *The Emergency Alert System (EAS) and All-Hazard Warnings*, Congressional Research Service (2010).....18

Lisa Eadicicco, *More People Now Shop on Amazon Using Smartphones and Tablets Than Computers*, Time (Dec. 28, 2015) 27

Lora Kolodny, *Passport Raises $8 Million To Help Cities Offer Pay-By-Mobile Parking, Transit*, TechCrunch (May 4, 2016) 28

Lorien C. Abroms, et al., *Text2Quit: Results From a Pilot Test of a Personalized, Interactive Mobile Health Smoking Cessation Program*, 17 J. Health Comm. 44 (2012) 34

Lyft, *Cities* 25

Mary Madden, et al., *Privacy, Poverty and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 Wash. U. L. Rev. 53 (2017).....35

Meryl Alper, Digital Youth with Disabilities (2014) 37

Meryl Alper, Giving Voice: Mobile Communication, Disability, and Inequality (2017).....36

Natalie Matthews, *Why Women Need Personal Safety Apps* (May 1, 2014).....20

NENA Public Education & PSAP Training Committee, *Public Education Plan* (2015).....20

NENA, 9-1-1 Statistics.....20

NENA, SMS Text-to-9-1-1 Resources for PSAPs & 9-1-1 Authorities.....20

Nick Corasaniti, *Elections to Be Easier for Voters With an App*, N.Y. Times (Aug. 6, 2013).....31

Nikita Stewart, *Applying for Food Stamps in New York? There's an App for That*, N.Y. Times (July 24, 2017).....39

Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 563 n.5 (2009).....6

Paul Krebs & Dustin T. Duncan, *Health App Use Among US Mobile Phone Owners: A National Survey*, 3 JMIR mHealth & uHealth e101 (2015) 34

Penny Crosman, *Banks Experiment with Apps for the Underbanked*, American Banker (Sept. 22, 2014) 36

Pew Charitable Trusts, *Online Voter Registration: Trends in Development and Implementation* (2015).....30, 31

Pew Research Center, *Internet/Broadband Fact Sheet* (Jan. 12, 2017).....15

Pew Research Center, *Mobile Fact Sheet* (Jan. 12, 2017) 6, 15, 35, 36

Press Release, *Ceridian's Dayforce Recruiting Platform Provides Seamless Access to More Talent Through Indeed* (May 23, 2017) 22

Press Release, *Congresswoman Kelly Leads Effort to Move Government Websites Into the 21st Century*, Website of Congresswoman Robin Kelly (May 9, 2017) 39

Press Release, *Glassdoor Improves Mobile Apps for iPad and iPhone Making Job Searching Easier* (June 23, 2016) 22

Radicati Group, *Email Statistics Report, 2015 – 2019* (2015) 23

Richard Ling, Taken for Grantedness: The Embedding of Mobile Communication into Society (2012) 16, 19

Robert Wood Johnson Foundation, *Health Policy Brief* 1–2 (2016) 33

Ryan Mac, *Square Makes Small Business Push for Growth Ahead of Earnings*, Forbes (Feb. 17, 2016) 27

Social Security Administration, *Digital Government Strategy* 39

Spyros Kitsiou et al., *Effectiveness of mHealth Interventions for Patients with Diabetes: An Overview Of Systematic Reviews*, 12 PLoS ONE 1 (March 2017) 34

Stacy Cowley, *Cash Faces a New Challenger in Zelle, a Mobile Banking Service*, N.Y. Times (June 12, 2017) 29

Stephen Blumberg & Julian Luke, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July - December 2016* (2017) 14

Taylor Soper, *Starbucks Mobile Order-Ahead Usage Doubles from Last Year, Now up to 8M Transactions per Month*, GeekWire (Apr. 21, 2016) 27

Teena Maddox, *Research: 74 Percent Using or Adopting BYOD*, ZDNet (Jan. 5 2015).....23

Universal Service Administration, *Do I Qualify?* 38

USCIS, *USCIS Website, E-Verify Now Optimized for Mobile Devices* (Feb. 29, 2016) 39

White House, Digital Government.....38

Constitutional Provisions

U.S. Const. amend. IV. 8

INTEREST OF *AMICI CURIAE*[1]

This case presents an important question about the application of the Fourth Amendment's protection against unreasonable searches in the context of cell site location information (CSLI). *Amici* are researchers and scholars who focus on the implications of technology on society, and we file this brief to help the Court consider how the third-party doctrine should be interpreted in the digital age.

Data & Society Research Institute is a nonprofit, nonpartisan, multidisciplinary research institute located in New York City. Researchers at Data & Society in the fields of sociology, anthropology, communications, media studies, computer science, and law study the social and cultural issues arising from data-driven technological development. Data & Society has an interest in seeing legal and policy rules informed by an accurate understanding of current social science. Because this case turns in part on questions related to the ubiquity and use of a particular technology in society—cellular telephones—Data & Society has an interest in informing this Court of the current state of related social science research.

Individual *amici* are leading scholars from various disciplines who study technology and society

---

[1] Both parties have filed with the Clerk of the Court letters of blanket consent to all *amicus* briefs under Rule 37.3. In accordance with Rule 37.6, no party's counsel authored this brief in whole or in part, and no one other than amici or their counsel made any financial contributions to the preparation or submission of this brief.

at U.S. and international institutions. The work of many of these scholars represents the state of the art in research on the social use and impact of mobile phone technology. *Amici* scholars have an interest in seeing law and policy accurately reflect their work and the work of their peers and their scholarly fields.

Technology and Society Scholars

Meryl Alper, Ph.D., Assistant Professor, Department of Communication Studies, Northeastern University; Faculty Associate, Berkman Klein Center for Internet & Society, Harvard University

Ifeoma Ajunwa, J.D., Ph.D., Assistant Professor, Cornell University, Industrial and Labor Relations School; Faculty Associate, Berkman Klein Center for Internet and Society, Harvard University

danah boyd, Ph.D., Principal Researcher, Microsoft Research; Founder and President, Data & Society Research Institute; Visiting Professor, Interactive Telecommunication Program, New York University

Gerard Goggin, Ph.D., Professor of Media and Communications, Department of Media and Communications, University of Sydney

Amy Gonzales, Ph.D., Assistant Professor, The Media School, Indiana University – Bloomington

Daniel Greene, Ph.D., Postdoctoral Researcher, Microsoft Research New England; Affiliate, Berkman Klein Center for Internet & Society, Harvard University

Lee Humphreys, Ph.D., Associate Professor, Department of Communication, Cornell University

Jeffrey Lane, Ph.D., Assistant Professor, Department of Communication, Rutgers, State University of New Jersey

Amanda Lenhart, Ph.D., Independent Researcher; Affiliate, Data & Society Research Institute

Richard S. Ling, Ph.D., Shaw Foundation Professor in Media Technology, Wee Kim Wee School of Communication and Information, Nanyang Technological University, Singapore

Karen Mossberger, Ph.D., Professor, School of Public Affairs, Arizona State University

Gina Neff, Ph.D., Associate Professor and Senior Research Fellow, Oxford Internet Institute and Department of Sociology, University of Oxford; Affiliate Associate Professor, Department of Communication & Department of Sociology, University of Washington

Desmond Upton Patton, Ph.D., Assistant Professor of Social Work, Columbia University; Fellow, Berkman Klein Center for Internet and Society, Harvard University

Julia Ticona, Ph.D., Postdoctoral Scholar, Data & Society Research Institute

Judy Wajcman, Ph.D., Anthony Giddens Professor of Sociology, London School of Economics

(Affiliations are for identification only)

at U.S. and international institutions. The work of many of these scholars represents the state of the art in research on the social use and impact of mobile phone technology. *Amici* scholars have an interest in seeing law and policy accurately reflect their work and the work of their peers and their scholarly fields.

Technology and Society Scholars

Meryl Alper, Ph.D., Assistant Professor, Department of Communication Studies, Northeastern University; Faculty Associate, Berkman Klein Center for Internet & Society, Harvard University

Ifeoma Ajunwa, J.D., Ph.D., Assistant Professor, Cornell University, Industrial and Labor Relations School; Faculty Associate, Berkman Klein Center for Internet and Society, Harvard University

danah boyd, Ph.D., Principal Researcher, Microsoft Research; Founder and President, Data & Society Research Institute; Visiting Professor, Interactive Telecommunication Program, New York University

Gerard Goggin, Ph.D., Professor of Media and Communications, Department of Media and Communications, University of Sydney

Amy Gonzales, Ph.D., Assistant Professor, The Media School, Indiana University – Bloomington

Daniel Greene, Ph.D., Postdoctoral Researcher, Microsoft Research New England; Affiliate, Berkman Klein Center for Internet & Society, Harvard University

Lee Humphreys, Ph.D., Associate Professor, Department of Communication, Cornell University

Jeffrey Lane, Ph.D., Assistant Professor, Department of Communication, Rutgers, State University of New Jersey

Amanda Lenhart, Ph.D., Independent Researcher; Affiliate, Data & Society Research Institute

Richard S. Ling, Ph.D., Shaw Foundation Professor in Media Technology, Wee Kim Wee School of Communication and Information, Nanyang Technological University, Singapore

Karen Mossberger, Ph.D., Professor, School of Public Affairs, Arizona State University

Gina Neff, Ph.D., Associate Professor and Senior Research Fellow, Oxford Internet Institute and Department of Sociology, University of Oxford; Affiliate Associate Professor, Department of Communication & Department of Sociology, University of Washington

Desmond Upton Patton, Ph.D., Assistant Professor of Social Work, Columbia University; Fellow, Berkman Klein Center for Internet and Society, Harvard University

Julia Ticona, Ph.D., Postdoctoral Scholar, Data & Society Research Institute

Judy Wajcman, Ph.D., Anthony Giddens Professor of Sociology, London School of Economics

(Affiliations are for identification only)

SUMMARY OF ARGUMENT

This case presents the question of how a Fourth Amendment doctrine developed decades ago should apply to modern technology. The so-called "third-party doctrine" states that voluntary conveyance of information to a third party extinguishes any legitimate expectation of privacy in that information. But the cases that form the doctrine extended an "assumption of the risk" rationale from earlier cases to sectors where information sharing was not truly voluntary: banking and telephone use. This Court should give more meaning to the voluntariness requirement of the third-party doctrine in the digital age.

An update to the third-party doctrine is vital in this case because neither ownership of a cell phone nor the sharing of cell site location information are meaningfully voluntary. Cell phones have replaced landlines as the nation's communications tools and have become part of the country's critical safety infrastructure. Cell phones are enabling better outcomes—and are often necessary—in employment, commerce, civic participation, and health. Vulnerable populations rely on cell phones even more than non-vulnerable populations, so a holding that cell phones obviate privacy would be doubly devastating for them. And the U.S. Government itself has in many instances recognized how vital cell phones are to Americans.

The third-party doctrine is ultimately a shorthand test for expectations of privacy that society would find reasonable. The vast majority of Americans carry cell phones that constantly transmit

passive location information. To hold that society finds it unreasonable to expect privacy in that information is effectively to deny privacy in contemporary life. This Court should limit the third-party doctrine so that it does not apply here.

ARGUMENT

This case lies at the intersection of two different lines of Fourth Amendment cases decided by this Court.

The first line, dating back four decades, yielded the third-party doctrine. That rule states that there is no legitimate expectation of privacy in information voluntarily conveyed to third parties. See *Smith* v. *Maryland*, 442 U.S. 735, 743–44 (1979); *United States* v. *Miller*, 425 U.S. 435, 442 (1976). In the second line, a majority of the Court has recognized that society's reliance on modern technology requires that traditional Fourth Amendment doctrines be updated to maintain the proper balance between law enforcement and privacy interests. See generally *Riley* v. *California*, 134 S. Ct. 2473 (2014); *United States* v. *Jones*, 565 U.S. 400 (2012); *Kyllo* v. *United States*, 533 U.S. 27, 33 (2001).

This case is in the same vein as *Jones* and *Riley*. *Amici* believe the Court should update the third-party doctrine in light of the realities of how modern technology works and the impact of that technology on society. If we find it unreasonable for a person to expect privacy in their movements over time because they—like 95% of society—use a cell phone, then we are unwilling to recognize privacy in the digital age at all.

I. THE THIRD-PARTY DOCTRINE SHOULD NOT APPLY TO CELL SITE LOCATION INFORMATION BECAUSE CELL PHONE USE IS NOT TRULY VOLUNTARY IN MODERN-DAY SOCIETY.

The third-party doctrine has long been controversial. See, *e.g.*, Gerald G. Ashdown, *The Fourth Amendment and the 'Legitimate Expectation of Privacy,'* 34 Vand. L. Rev 1289, 1315 (1981); Lewis R. Katz, *In Search of A Fourth Amendment for the Twenty-First Century*, 65 Ind. L.J. 549, 564 (1990); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1138 (2002); see also Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 563 n.5 (2009) ("A list of every article or book that has criticized the doctrine would make this the world's longest law review footnote.")

Relying on the doctrine, the Government argues that despite the passivity with which CSLI is conveyed to cell carriers, Carpenter—and the 95% of Americans who own cell phones, Pew Research Center, *Mobile Fact Sheet* (Jan. 12, 2017) (hereinafter, *Mobile Fact Sheet*)[2]—voluntarily convey vast amounts of their historical location information to their cell carriers. See BIO, *passim* (using and quoting the word "voluntarily" sixteen times in describing precedent and relating it to the transfer of CSLI to the cellular providers). According to the Government, this means police should be able to obtain CSLI without a warrant.

---

[2] http://www.pewinternet.org/fact-sheet/mobile (all Internet materials last visited Aug. 9, 2017).

This argument should not win the day because there is no volitional act of transmission. As this Court has observed, cell phones have become "a pervasive and insistent part of daily life." *Riley*, 134 S. Ct. at 2484. The 95% of Americans with cell phones all passively transmit data about their locations while their phones are powered on. This conveyance is not a truly "voluntary" act. Cell phone users should not be said to assume the risk that the government will track their movements simply because they carry a cell phone.

The implications of the third-party doctrine are particularly far-reaching as society embraces new technologies such as cell phones, cloud computing, and other data services. As JUSTICE SOTOMAYOR suggested in *Jones*, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." 565 U.S. at 417 (SOTOMAYOR, J., concurring). The Court should reject the argument that the third-party doctrine applies to CSLI by giving the volitional requirement more substance and recognizing that CSLI transmission is not voluntary.

A. The Court Should Adapt the Third-Party Doctrine for the Digital Age by Giving More Substance to the Voluntary Conveyance Requirement.

The Fourth Amendment commands that "|t|he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated[.]" U.S. Const. amend. IV. A Fourth Amendment search occurs when "the government violates a subjective

expectation of privacy that society recognizes as reasonable." *Kyllo*, 533 U.S. at 33 (2001); *Katz* v. *United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

The third-party doctrine is a shorthand rule about what privacy interests we as a society find "reasonable." The rationale underlying the doctrine is that people cannot reasonably expect privacy in information they willingly choose to convey to another. By deciding to expose that information, they assume the risk that it will be disclosed to the government. *Smith*, 442 U.S. at 744-45; *Miller*, 425 U.S. at 443.

In the context of CSLI, there are two ways to claim that the transmission of data to phone carriers is voluntary. First, CSLI could be offered voluntarily if the user could opt whether to transmit CSLI, given cell phone ownership and use. Second, CSLI may be transmitted voluntarily if cell phone ownership and use is a truly voluntary choice.

In their brief in support of certiorari, the Electronic Frontier Foundation and other civil society groups addressed the first question. Brief for Electronic Frontier Foundation, et al. as *Amici Curiae* in Support of Certiorari at 6-12, 21. As they explained, CSLI is generated passively and unknowingly, "whenever [cell phones] are on and searching for a signal." *Id.* at 21. The acts of going to a bank (*Miller*) and dialing a phone number (*Smith*) are at least nominally volitional in a way that passive transmission of CSLI is not. CSLI travels between a powered-on phone and cell tower, whether the user means for it to happen or not. To the extent that the voluntariness claim relies on a concrete

volitional act of sending information, this case is distinguishable from *Miller* or *Smith*.

The other possible argument is that having a cell phone and turning it on is a voluntary act sufficient to trigger the third-party doctrine. But that cannot be true for anything but the thinnest conception of voluntariness. As this Court has recognized, cell phones have become central to modern society. See *Riley*, 134 S. Ct. at 2484; *City of Ontario* v. *Quon*, 560 U.S. 746, 760 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."). Having a cell phone is necessary the same way having a car is necessary in most parts of the country.

B. The Third-Party Doctrine's Foundational Cases Predating *Miller* and *Smith* Support a More Robust Notion of Voluntary Conveyance.

While the third-party doctrine has voluntary conveyance at its core, from its inception it has given the concept of voluntariness short shrift. In *Miller*, the Court held that there was no privacy interest in banking information that was "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." 425 U.S. at 442. But as Justice Brennan pointed out in his dissenting opinion, giving financial information to a bank was not meaningfully voluntary: "For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary

society without maintaining a bank account." *Id.* at 451 (Brennan, J., dissenting).

The case law prior to *Miller* did not require such a hollow interpretation of voluntariness. *Miller* relied on a line of cases that dealt with legitimately voluntary disclosures. For example, in *Hoffa* v. *United States*, 385 U.S. 293 (1966), the police turned an associate of Jimmy Hoffa's against him in exchange for dropping the charges. The defendant had disclosed information freely to a third party, not expecting the third party to offer it to the police. The Court held that there was no Fourth Amendment violation because the speaker assumed the risk of disclosure: "[T]he Fourth Amendment [does not] protect[] a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it." *Id.* at 303.

Five years later, the Court held in *United States* v. *White*, 401 U.S. 745 (1971), that an informant's wearing of a wire did not change the analysis, holding that "one contemplating illegal activities must realize and risk that his companions may be reporting to the police." *Id.* at 752; see also *Lopez* v. *United States*, 373 U.S. 427, 439 (1963) (holding Fourth Amendment was not violated when informant was wearing a wire used for recording rather than instant transmission). To craft what would become the third-party doctrine, *Miller* borrowed this assumption-of-the-risk rationale and extended it to a basic functionality of society: doing business with a bank. 425 U.S. at 443. *Smith* then extended the reasoning to the telephone system, another basic functionality of society. 442 U.S. at 744.

The informant cases dealt with actual voluntary disclosures to a third party in a way that neither *Miller* nor *Smith* ever did. For that reason, recognizing that today's cell phone use is not meaningfully voluntary need not abrogate the entire third-party doctrine. Though Justice SOTOMAYOR was certainly correct when she wrote that the third-party doctrine is "ill suited to the digital age," *Jones*, 565 U.S. at 417 (SOTOMAYOR, J., concurring), this case can be resolved without overturning the doctrine entirely by giving more substance to the voluntariness requirement.

C. The Fourth Amendment's Content/Non-Content Distinction Does Not Solve the Third-Party Doctrine's Problems.

The court below suggested that the traditional Fourth Amendment distinction between "content" and "non-content" information resolves the problems presented by the third-party doctrine. 819 F.3d 880, 887 (6th Cir. 2016) (drawing a distinction between *Katz* and *Smith* because a wiretap captures the content of calls but a pen register does not).

But the content/non-content rationale does not make the third-party doctrine workable for two reasons. First, it is not clear in a world of data aggregation what is content and non-content. A single point of data about a person might not expose much about their life. But many data points together can reveal more sensitive information: activities, associations, habits, and other patterns. As the Court recognized in *Riley* and several Justices recognized in *Jones*, a large quantity of data may disclose private details about a person that a small amount of data

cannot. *Riley*, 134 S. Ct. at 2489 ("The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet."); *Jones*, 565 U.S. at 430 (ALITO, J., concurring) ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4–week mark.").

Second, the content/non-content distinction is not what the third-party doctrine cases say. While *Smith* did draw a distinction between contents of a phone call and the phone numbers dialed, the relevant legal distinction for the rule applied by the Court was between what the pen register actually acquired—that is, what was shared with a third party—and what was kept private. 442 U.S. at 741 ("[A] pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications.") (emphasis in original). If the same distinction is applied to communications and files that people disclose to third-party service providers, it is not at all clear that individuals would have a legitimate expectation of privacy in the content they choose to share with a service provider.

Miller goes even farther, expressly saying that the contents of bank documents are fair game under the third-party doctrine: "All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." 425 U.S. at 442. This

formulation of the rule is deeply unsettling in an age when people increasingly store their most private photos, videos, messages, professional files, associations, and other information with third-party providers. If the third-party doctrine applies in the way *Miller* and *Smith* suggest, the Government would not need a warrant to gather any of this information. That is an untenable outcome.

The court need not resort to the content/non-content distinction to resolve this tension. It can be addressed by making the third-party doctrine more nuanced. The disclosure should only count as voluntary if the primary purpose of the sharer is to communicate the information to that particular recipient. That is what distinguishes *Hoffa* and *White* from *Smith and Miller*: the assumption of the risk comes with sharing a piece of information for no purpose other than sharing the information. If the sharing is instead a byproduct of using services, then it is not voluntary the same way. For example, if a person emails a message to someone's Google email address, that message should be protected by the Fourth Amendment despite Google's ability to access it. The sender is transmitting the message to Google for the purpose of conveying information to someone else. Google is simply acting as an intermediary to transfer the message from one person to another. Google is not a recipient of a communication, but a provider of a service. But if the same person emails a message to Google for the purpose of communicating with Google itself, then Google can disclose that message to the police with no Fourth Amendment implications. The difference is not content versus non-content, but rather the sender's decision to

voluntarily disclose information to a particular recipient.

II. THE USE OF CELL PHONES IN THE MODERN WORLD IS NOT MEANINGFULLY VOLUNTARY.

Cell phones are not a voluntary convenience in modern society. Every day, cell phones become more essential to fulfill basic needs such as communications with family, safety, health, employment, commerce, civic participation, and government services. It is impossible to square the centrality of modern cell phones to daily life with the notion that using one amounts to a waiver of Fourth Amendment rights in the data transmitted by them.

A. Cell Phones Are Necessary to Participate in the Most Basic Aspects of Everyday Social and Family Life.

Cell phones are now part of society's basic infrastructure. The most important reason why cell phones are indispensable may be the most obvious: they are our phones. More than half of all households in the U.S. have a cell phone but no landline. Stephen J. Blumberg & Julian V. Luke, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July - December 2016* (2017).[3] In 2016, more than seven of ten adults aged 25–29 (72.7%) and 30-34 (71%) lived in households with only wireless telephones. *Id.* at 2. Over 60% of children and those aged 18–24 live in cell phone-only households. *Id.* at 1–2. Cell phone

[3] https://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201705.pdf.

ownership is nearly at population saturation. See *Mobile Fact Sheet.*

Cell phones are also increasingly the way that people access the internet. As internet access has become more central to participation in daily life, Americans use smartphones more than any other device to access the internet, even at home. *Id.* While many smartphone owners have difficulty with cell service at least occasionally, Aaron Smith, Pew Research Center, *U.S. Smartphone Use in 2015* at 52 (2015) (hereinafter, *U.S. Smartphone Use in 2015*),[4] mobile use of the internet continues to grow. *Mobile Fact Sheet.* And while cell phone ownership has increased consistently, ownership of laptop and desktop computers has remained relatively flat. *Id.* Since 2011, smartphone ownership in particular has increased by 8.4% per year, *id*, and broadband internet subscriptions remain relatively flat. Pew Research Center, *Internet/Broadband Fact Sheet* (Jan. 12, 2017).[5] Twelve percent of Americans own a smartphone, but do not have traditional broadband service at home. *Mobile Fact Sheet.*

According to Richard Ling, a communications scholar and expert on mobile communication, "the mobile phone moved from being useful to becoming essential, and is now taken for granted." Richard Ling, Taken for Grantedness: The Embedding of Mobile Communication into Society 157 (2012) (hereinafter, Taken for Grantedness). He writes that cell phones "ha[ve] restructured how we coordinate

---

[4] http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/03/PI_Smartphones_0401151.pdf.
[5] http://www.pewinternet.org/fact-sheet/internet-broadband.

our lives, keep ourselves safe, and organize our family." *Id.* at 124.

Other experts concur. As early as 2004, Christian Licoppe, a sociologist of information and communication, referred to the social changes that came from ubiquitous cell phones as "connected presence," arguing that there has been a "gradual shift in which communication technologies . . . are exploited to provide a continuous pattern of mediated interactions" that "[blur] the boundaries between absence and presence." Christian Licoppe, *'Connected' Presence: The Emergence of a New Repertoire for Managing Social Relationships in a Changing Communication Technoscape*, 22 Env. & Planning D: Soc'y & Space 135, 135–36 (2004). Judy Wajcman, a sociologist of digital technologies, explains that in today's world, "constant connectivity is the norm," and we have rearranged the way we structure our lives as a result. Judy Wajcman, Pressed for Time: The Acceleration of Life in Digital Capitalism, 10–11 (2014). As Ling observed, the use of mobile phones is no longer "simply a matter of personal choice; it is in general an assumed part of social interaction." Taken for Grantedness at 7.

Cell phones are especially significant for young people. Pew Research reports that 88% of teens have either a smartphone (73%) or a cell phone (15%). Amanda Lenhart, et al., Pew Research Center, *Teens, Technology, and Friendships* 10 (2015).[6] Overall, mobile phone based communication is the most important way teens communicate with their friends.

---

[6] http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/08/Teens-and-Friendships-FINAL2.pdf.

Eighty-eight percent text with their friends, (55% on a daily basis), 69% maintain relationships through phone calls, and 66% use social media (which itself is usually accessed via mobile). *Id.* at 3.

Family interactions have become dependent on cell phones as well. According to several scholars, "[o]ne of the most distinctive features of the mobile phone is its use for the microcoordination of family arrangements and schedules." Judy Wajcman, Michael Bittman & Judith Brown, *Families without Borders: Mobile Phones, Connectedness and Work-Home Divisions*, 42 Sociology 635, 636 (2008) (citations omitted). They suggest that this may be the reason cell phones became so popular, so quickly. *Id.* Cell phones also help families that are physically separated stay in touch. A 2006 survey of parents found that 90% of respondents said they use mobile phones to stay in touch with their children in college. College Parents of America, *Survey of Current College Parent Experiences* (2006).

B. Cell Phones Are Essential Public Safety Infrastructure and Personal Safety Equipment.

Because cell phones are ubiquitous, they have become a major part of public safety infrastructure. The original Emergency Alert System (EAS) was built in the 1950s to transmit emergency messages using over-the-air broadcasting technology. Linda K. Moore, *The Emergency Alert System (EAS) and All-Hazard Warnings*, Congressional Research Service, Summary (2010). Now jointly administered by the Federal Emergency Management Agency (FEMA), the Federal Communications Commission (FCC), the National Weather Service (NWS), it has been

updated to use Cell Broadcasting Services, which push alerts directly to cell phones. *Id.* These include direct presidential alerts, imminent threats to life and safety, and AMBER alerts, which provide information about abducted children. *Id.* at 10. In short, the federal government sends emergency information directly to cell phones because they are a reliable and effective way to reach the general public.

Cell phones are also key tools in natural disasters. Weather apps that rely on NWS data, including one created by NOAA, can push emergency alerts for severe weather and aid in evacuation. Once a disaster occurs, people use whatever means they have at hand to get help. In 2010, the Red Cross surveyed 1,058 adults about their use of social media in emergency situations, finding "if they needed help and couldn't reach 9-1-1, one in five would try to contact responders through a digital means such as e-mail, websites or social media." American Red Cross, *Social Media Grows Up – Red Cross Emergency Social Data Summit* (Aug. 12, 2010).[7] And "[i]f web users knew of someone else who needed help, 44 percent would ask other people in their social network to contact authorities, 35 percent would post a request for help directly on a response agency's Facebook page and 28 percent would send a direct Twitter message to responders." *Id.*

Facebook's Safety Check feature allows people in disaster areas to alert loved ones that they are safe. While 52.4% of global Facebook users access the site exclusively through a mobile device, Emil Protalinski, *Facebook Passes 1.65 Billion Monthly*

---

[7] http://www.redcross.org/news/article/Social-Media-Grows-Up--Red-Cross-Emergency-Social-Data-Summit.

Active Users, 54% Access the Service Only on Mobile, VentureBeat (Apr. 27, 2016),[8] the number is likely much higher in an emergency situation. In 2015, a Pew Research Study found that 53% of smartphone owners "have been in an emergency situation where having their phone available helped resolve the situation." *U.S. Smartphone Use in 2015* at 25. As more people rely on social media to communicate information, others will know to go there to receive it; that is why Safety Check is effective. This expectation then reinforces the need for people to have cell phones to communicate in emergencies. See Taken for Grantedness at 94 ("[W]e collectively gain value from the system since . . . the more people there are who own a mobile phone, the better we are able to maintain social contact.").

People in smaller scale emergencies also turn to cell phones. According to the National Emergency Number Association (NENA), there are "an estimated 240 million calls made to 9-1-1 each year," of which "70% or more are made from wireless devices." NENA, 9-1-1 Statistics.[9] The 9-1-1 industry is also working with wireless carriers and the FCC to implement texting to 9-1-1 throughout the country. See NENA, SMS Text-to-9-1-1 Resources for PSAPs & 9-1-1 Authorities.[10] Text to 9-1-1 is projected to close gaps in service to people who have speech disabilities or are deaf, victims of domestic violence, or non-native English speakers. NENA Public

---

[8] https://venturebeat.com/2016/04/27/facebook-passes-1-65-billion-monthly-active-users-54-access-the-service-only-on-mobile.

[9] https://www.nena.org/?page=911Statistics.

[10] http://www.nena.org/?page=textresources.

Education & PSAP Training Committee, *Public Education Plan* 9 (2015).[11]

Mobile phones are also an important means of ensuring personal safety, especially among women. Some mobile apps function as panic buttons that send an alert to select contacts. Natalie Matthews, *Why Women Need Personal Safety Apps*, Elle (May 1, 2014).[12] In a 2012 survey, college-aged women deemed mobile phones to be more effective than pepper spray for ensuring their personal safety. Kathleen M. Cumiskey & Kendra Brewster, *Mobile Phones or Pepper Spray? Imagined Mobile Intimacy as a Weapon of Self-Defense for Women*, 12 Feminist Media Stud. 590, 594 (2012). And apps such as "I'm Getting Arrested," "Hands Up 4 Justice," and "Stop and Frisk Watch" are aimed at over-policed populations such as African-American men and offer similar capacities. Alessandra Ram, *It's Your Right to Film the Police. These Apps Can Help*, Wired (May 3, 2015).[13]

A decision not to have a cell phone is therefore a decision not to own a device that increases personal safety, not to own a device that allows loved ones to contact or find you in an emergency, and not to participate in a system that enhances public safety for all. Such connections are not a luxury.

---

[11] http://c.ymcdn.com/sites/www.nena.org/resource/resmgr/Standards/NENA-REF-003.1-2015_Texting_.pdf.

[12] http://www.elle.com/culture/tech/news/a14941/womens-safety-apps.

[13] https://www.wired.com/2015/05/right-film-police-apps-can-help.

C. Cell Phones Are Both Necessary to Find Employment and an Important Part of Workplace Infrastructure.

Today Americans find their jobs on the internet. According to a 2015 Pew Research Study, "a majority of U.S. adults (54%) have gone online to look for job information, [and] 45% have applied for a job online." Aaron Smith, Pew Research Center, *Searching for Work in the Digital Era* 2 (2015) (hereinafter, *Searching for Work*).[14] For Americans between the ages of 18 and 29, those numbers jump to 83% researching jobs online, and 79% applying. *Id.* at 10. Seventy-nine percent of Americans who applied for a job in the two years prior to the study used internet resources to do so, and 34% say these resources were the most important tool they used. *Id.* at 2. In fact, a recent survey showed that, barring job applicants that receive accommodation for disabilities, the top 20 Fortune 500 employers "all require job applications to be submitted online." Daniel Greene & Ifeoma Ajunwa, *Automated Hiring Platforms as Technological Intermediaries and Brokers* at 1 (unpublished manuscript).[15]

Job searching happens not just on the internet, but specifically on mobile phones. Twenty-eight percent of Americans, including more than half of those between ages 18 and 29, have used a smartphone to look for employment. *Searching for*

---

[14] http://assets.pewresearch.org/wp-content/uploads/sites/14/2015/11/PI_2015-11-19-Internet-and-Job-Seeking_FINAL.pdf.

[15] http://dmgreene.net/wp-content/uploads/2014/11/GreeneAjunwaAutomated-Hiring-Plaforms-as-Technological-Intermediaries-and-Brokers.pdf.

Work at 3. These strategies are not limited to the youngest demographic either. Nearly 40% of 30- to 49-year-olds have looked for work using their smartphones. *Id.* at 17. The leading job recruiting websites are reporting that their traffic comes primarily from mobile devices. Press Release, *Ceridian's Dayforce Recruiting Platform Provides Seamless Access to More Talent Through Indeed* (May 23, 2017) (60% of Indeed's 200 million unique visitors per month from mobile)[16]; Press Release, *Glassdoor Improves Mobile Apps for iPad and iPhone Making Job Searching Easier* (June 23, 2016) (more than 50% of monthly visits from mobile).[17]

In addition to being necessary for job-hunting, mobile phones are often part of workplace infrastructure, and people in such jobs cannot refuse to have a cell phone. Market research estimates that the use of e-mail for business related communication has grown steadily over the past two years (3% per year), Radicati Group, *Email Statistics Report, 2015 – 2019* at 4 (2015),[18] and for the 59% of Americans who occasionally work outside of their "home base" workplace, 50% say the internet & cell phones are "very important" for allowing them to do their jobs remotely. Kristen Purcell & Lee Rainie, Pew Research Center, *Technology's Impact on Workers* 8

---

[16] http://www.marketwired.com/press-release/ceridians-dayforce-recruiting-platform-provides-seamless-access-more-talent-through-2217809.htm.

[17] https://www.glassdoor.com/press/glassdoor-improves-mobile-apps-ipad-iphone-making-job-searching-easier.

[18] http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf.

(2014).[19] Gallup estimated in 2014 that "80% of full-time U.S. workers ha[d] a smartphone with Internet access," Jim Harter et al., *Most U.S. Workers See Upside to Staying Connected to Work*, Gallup (Apr. 30, 2014),[20] and market research estimates that 74% of companies have "bring your own device" policies that allow employees to use their personal devices for work. Teena Maddox, *Research: 74 Percent Using or Adopting BYOD*, ZDNet (Jan. 5, 2015).[21]

Many hourly jobs use on-call scheduling, a practice in which employees are required to call in to their workplace several hours before a shift starts to find out if they are needed. And recent estimates suggest that up to 90% of retail workers are subject to last-minute scheduling changes, Daniel Schneider & Kristen Harknett, *Schedule Instability and Unpredictability and Worker and Family Health and Wellbeing* (2016) (working paper),[22] which implicitly require that the worker be reachable by phone at all times. Many of these scheduling practices rely on a host of worker-facing scheduling apps, such as When I Work (which boasts over 100,000 enterprise customers), Zip Schedules, Sling, HotSchedules, TrackSmart, and Schedulehead. Twenty thousand workers at large retailers such as Starbucks,

---

[19] http://assets.pewresearch.org/wp-content/uploads/sites/14/2014/12/PI_Web25WorkTech_12.30.141.pdf.

[20] http://www.gallup.com/poll/168794/workers-upside-staying-connected-work.aspx.

[21] http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod.

[22] http://cdn.equitablegrowth.org/wp-content/uploads/2016/09/12135618/091216-WP-Schedule-instability-and-unpredictability.pdf.

McDonalds, and Old Navy use Shyft, an app that allows them to swap shifts with co-workers. Dina Bass, *New App Helps Shift Workers Swap Hours*, Boston Globe (July 13, 2016).[23]

Finally, so-called "gig economy" work has smartphone apps at its core. Ride-hailing services such as Uber and Lyft require their workers and customers to use smartphone apps to engage with the service. In 2014, Uber had 160,000 drivers signed up in the U.S. Jonathan Hall & Alan Krueger, *An Analysis of the Labor Market for Uber's Driver-Partners in the United States*, at 1 (2015).[24] Though Lyft's employment numbers are unavailable, it operates in 550 cities nationwide. Lyft, *Cities*.[25] The gig economy also includes services such as child and elder care (*e.g.*, care.com), house cleaning (*e.g.*, Handy), and catchall everyday tasks (*e.g.*, TaskRabbit). Cell phones are essential for people looking for work through these on-demand apps and the income is critical for many. Of the nearly 1 in 10 Americans that have earned income from on-demand labor apps, Pew has reported that 60% say the income they generate through them is "essential or important to their overall financial situation." Aaron

---

[23] https://www.bostonglobe.com/business/2016/07/13/starbucks-baristas-want-better-hours-there-app-for-that/AXpGcIqA36Mcoc1udDJfVP/story.html.

[24] https://s3.amazonaws.com/uber-static/comms/PDF/Uber_Driver-Partners_Hall_Kreuger_2015.pdf.

[25] https://www.lyft.com/cities.

Smith, Pew Research Center, *Labor Platforms: Technology-Enabled 'Gig Work'* 4 (2016).[26]

Cell phones are already an integral part of looking for and carrying out work for a wide-spectrum of high and low-income workers. The acquisition and rapid development of mobile apps for the workplace suggest that cell phones will become more, not less important to the labor market in years to come, as many jobs become more flexible and traditional employment relationships change. The increasing importance of these technologies to lower-income Americans to secure their livelihoods suggests that economic necessity makes cell phones necessary, not voluntary.

D. Cell Phones Are Widely Used for Commerce and Banking and Are Rapidly Becoming Integral.

Commerce is rapidly becoming the province of the smartphone. Mobile payment apps—which store credit card information and interact with wireless readers in stores and in some apps—now come by default on most cell phones. Devindra Hardawar, *Google Wallet to Come Pre-Installed on Phones for Major Carriers*, Engadget (Feb. 23, 2015).[27] According to the Federal Reserve Board, 47% of smartphone owners made at least one mobile payment in 2014. Federal Reserve Board, *Consumers*

---

[26] http://assets.pewresearch.org/wp-content/uploads/sites/14/2016/11/17161707/PI_2016.11.17_Gig-Workers_FINAL.pdf

[27] https://www.engadget.com/2015/02/23/google-wallet-softcard-deal.

and Mobile Financial Services 2015 at 16 (2015).[28] Several technology companies aim to replace wallets entirely. See Brian Barrett, *Your Phone Will Replace Your Wallet at the ATM, Too*, Wired (Jan. 28, 2016).[29]

Many retailers are creating and popularizing their own in-store payment apps. For example, in the first quarter of 2016, 24% of all Starbucks transactions in the U.S. were paid through Starbucks' mobile app. Taylor Soper, *Starbucks Mobile Order-Ahead Usage Doubles from Last Year, Now up to 8M Transactions per Month*, GeekWire (Apr. 21, 2016).[30] Mobile devices are even involved in traditional credit card transactions. Many small businesses without much infrastructure (*e.g.*, food trucks) would not exist without Square, a company that provides credit card readers that connect to smartphones or tablets, and allow businesses to process and track payments through their mobile app, Square Cash. See Ryan Mac, *Square Makes Small Business Push for Growth Ahead of Earnings*, Forbes (Feb. 17, 2016).[31]

Mobile wallets and in-store payment apps do not tell the whole story. E-commerce is moving to mobile as well. During the 2015 holiday season, nearly 70% of Amazon customers placed orders on a mobile device, and over 70% of Wal-Mart's website traffic—leading to 50% of purchases—came from

---

[28] https://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf.

[29] https://www.wired.com/2016/01/cardless-atms.

[30] https://www.geekwire.com/2016/starbucks-mobile-order-ahead-usage-doubles-last-year-now-8m-transactions-per-month.

[31] https://www.forbes.com/sites/ryanmac/2016/02/17/square-small-business-payroll-capital-transition/#29411c237fc7.

mobile. Lisa Eadicicco, *More People Now Shop on Amazon Using Smartphones and Tablets Than Computers*, Time (Dec. 28, 2015).[32] Surely that number is higher now.

The transition of commerce to mobile apps extends far beyond retail. Take transportation, for example. Most major U.S. airlines—including Delta, JetBlue, Southwest, United, and Virgin America—offer check-in via mobile app. Companies like Passport have entered into government partnerships in various cities to provide pay-by-mobile apps for parking meters and other public transportation, such as ParkBoston and ParkChicago. Lora Kolodny, *Passport Raises $8 Million To Help Cities Offer Pay-By-Mobile Parking, Transit*, TechCrunch (May 4, 2016).[33] Mobile mapping apps are ubiquitous; as of 2016, Google's app had 95.3 million global users and Apple's had 60.3 million. ComScore, *The 2016 U.S. Mobile App Report* 32 (2017).[34]

Banking is another sector increasingly reliant on mobile. Most banks have apps, which allow for checking balances, making payments, and mobile check deposits. According to an FDIC study, in 2015, 31.9% of banked households used mobile apps, up from 23.3% in 2013. FDIC, *2015 FDIC National Survey of Unbanked and Underbanked Households* 24 (hereinafter, *FDIC Study*).[35] As Nessa Feddis of

---

[32] http://time.com/4162188/amazon-holiday-shopping-statistics-2015.

[33] https://techcrunch.com/2016/05/04/passport-raises-8-million-to-help-cities-offer-pay-by-mobile-parking-transit.

[34] https://www.comscore.com/Insights/Presentations-and-Whitepapers/2016/The-2016-US-Mobile-App-Report.

[35] https://www.fdic.gov/householdsurvey/2015/2015report.pdf.

the American Bankers Association observed, "[p]eople are receiving checks less frequently, but when they do they're increasingly turning to mobile banking to deposit them." American Bankers Association, *Survey: More Americans Using Mobile Deposit* (2015).[36] Unsurprisingly, what has replaced the physical check are more mobile payment apps. Whether paying for services, rent, or a portion of last night's dinner out, people are using mobile payment apps such as Venmo—which processes $20 billion in payments per year, Leena Rao, *Venmo Is On Track to Process $20 Billion in Payments Per Year*, Fortune (Oct. 20, 2016)[37]—as well as PayPal, Google Wallet, and Zelle, a mobile service launched in June by big banks to compete with Venmo. Stacy Cowley, *Cash Faces a New Challenger in Zelle, a Mobile Banking Service*, N.Y. Times (June 12, 2017).[38]

E. Cell Phones Have Become a Key Technology for Civic Participation.

A 2017 study of internet users in Chicago found that people who have mobile access to the internet are more likely to engage in civic activities than those who do not have mobile access. Karen Mossberger, Caroline J. Tolbert & Christopher Anderson, *The Mobile Internet and Digital Citizenship in African-American and Latino Communities*, 20 Info. Comm. & Soc'y 1587, 1597 (2017). The study found that for African Americans and Latino populations specifically, having access to

---

[36] http://www.aba.com/Press/Pages/082515MobileBankingSurvey.aspx.

[37] http://fortune.com/2016/10/20/venmo-20-billion.

[38] https://www.nytimes.com/2017/06/12/business/dealbook/mobile-banking-zelle-venmo-apple-pay.html.

mobile internet has positive effects on the likelihood that they will engage in civic activities online, including "searching for neighborhood information, use of the City of Chicago website, use of Facebook and Twitter for civic information, searching for information about politics, accessing government information or reading online news." *Id.* at 1596–97.

Mobile phones are also how people get their news. A Knight Foundation study on how people use phones to access information found that "social networking apps on mobile compete as a news source with other media forms trailing only TV but pulling ahead of radio, newspapers and magazines among social networkers." Knight Foundation, *Mobile-First News: How People Use Smartphones to Access Information* 10 (2016).[39] According to the Nielsen Electronic Mobile Measurement Panel (which Knight cites), 89% of the adult U.S. mobile population access news and information through their mobile device. *Id.* at 4.

Lack of access to a cell phone may reduce an individual's opportunities for political participation on both a local and national level. For example, online voter registration first became available in Arizona in 2002, and as a result, voters registered online rose from 25% in 2003 to 39% in 2008. Holly Maluk, Myrna Pérez & Lucy Zhou, Brennan Center for Justice, *Voter Registration in a Digital Age: 2015 Update* 13 (2015).[40] By 2014, online voter

---

[39] https://kf-site-production.s3.amazonaws.com/publications/pdfs/000/000/187/original/Topos_KF_Mobile-Report_Final_052616.pdf.

[40] https://www.brennancenter.org/publication/voter-registration-digital-age-2015-update.

registration had become available in 20 states. Pew Charitable Trusts, *Online Voter Registration: Trends in Development and Implementation* 2 (2015).[41] Voters are increasingly registering through mobile-optimized websites that people access with smartphones. *Id.* Major projects aimed at boosting voter participation have focused on mobile phones as an avenue for reaching eligible voters, by, for example, providing information on polling place locations and ballot information.

In 2013, the New York City Campaign Finance Board launched NYC Votes, a mobile app designed to encourage political participation by allowing people to begin voter registration, monitor their registration status, and receive information, such as the ability to look up local candidates. Nick Corasaniti, *Elections to Be Easier for Voters With an App*, N.Y. Times (Aug. 6, 2013).[42]

The Voter Information Project, a joint effort from The Pew Charitable Trusts, Google, and state and local officials, has created a mobile app that provides polling place, ballot, and candidate information. Jen Tolentino, Voting Information Project, *VIP Offers Free iOS App* (June 24, 2014).[43] Relatedly, the Obama campaigns showed that mobile devices could be "a powerful tool for political campaigns by centralizing canvassing and fundraising innovations." Encyclopedia of Social Media and Politics 899 (Kerric Harvey, ed. 2014).

---

[41] http://www.pewtrusts.org/~/media/assets/2015/05/ovr_2015_brief.pdf.

[42] http://www.nytimes.com/2013/08/07/nyregion/registration-as-a-voter-to-be-easier-via-phone.html.

[43] https://votinginfoproject.org/news/vip-offers-free-ios-app.

Outside of elections, government agencies have invested in mobile apps that provide services, information, and other resources. An online Federal Government Mobile Apps Directory lists 338 mobile apps that include "government native apps, hybrid apps, responsive sites, and mobile websites that offer official information and services in the palm of your hand." Federal Government Mobile Apps Directory, USA.gov.[44] Several major cities, including Boston, New York, Philadelphia, Chicago and Los Angeles have created mobile app versions of 311 service requests, where residents can report city maintenance issues like potholes and graffiti. See, *e.g.*, City of Boston Apps, City of Boston.[45]

These trends are likely to intensify. As budgets shrink and funding is cut, governments will employ fewer people attending to lines and fewer people answering phones. Government, like the private sector, will often turn to technology as a less expensive substitute for labor, using apps to directly interact with citizens. As government moves to mobile more every day, those without cell phones will miss out on crucial services.

F. Cell Phones Are Enabling Better Health Outcomes.

Many people with chronic illnesses must maintain contact with physicians and loved ones to manage their conditions. For them, being without a mobile phone could be seriously detrimental to health outcomes, even deadly. See generally Amy L.

---

[44] https://www.usa.gov/mobile-apps.

[45] https://www.boston.gov/departments/innovation-and-technology/apps.

Gonzales, *Health Benefits and Barriers to Cell Phone Use in Low-Income Urban U.S. Neighborhoods: Indications of Technology Maintenance*, 2 Mobile Media & Comm. 233 (2014) (hereinafter, *Health Benefits and Barriers to Cell Phone Use*). In a recent interview-based study, mobile phones were such an important resource for low-income patients managing HIV that researchers found "nearly all clients viewed the cell phone as a primary necessity"—so much that some re-organized their budgets for essentials like food and gas in order to keep their phones in operation. Amy L. Gonzales, Lindsay Ems & Venkata Ratnadeep Suri, *Cell Phone Disconnection Disrupts Access to Healthcare and Health Resources: A Technology Maintenance Perspective*, 18 New Media & Soc'y 1422, 1429 (2016) (hereinafter, *Cell Phone Disconnection Disrupts Access*).

According to the Robert Wood Johnson Foundation, 20% of Americans live in rural areas, but only 9% of physicians practice there. Robert Wood Johnson Foundation, *Health Policy Brief* 1–2 (2016).[46] Still a nascent industry, telehealth allows people in these areas without ready access to doctors to get diagnoses, interact in real-time video, and have remote patient monitoring. *Id.* at 1–2. While telehealth encompasses more than mobile phones, investment is pouring in for mobile applications. See Bill Siwicki, *American Well Partners With Samsung Electronics For Mobile Telehealth*, Healthcare IT

[46] http://healthaffairs.org/healthpolicybriefs/brief_pdfs/healthpolicybrief_162.pdf.

News (Feb 21, 2017).[47] And initial research of remote health monitoring is promising for health outcomes. See Spyros Kitsiou et al., *Effectiveness of mHealth Interventions for Patients with Diabetes: An Overview Of Systematic Reviews*, 12 PLoS ONE 1 (March 2017).

Mobile phones are also being used to intervene in health outcomes. A survey of smartphone users found that 58% have downloaded a mobile health app, primarily for fitness and nutrition tracking, and most of those people use them daily. Paul Krebs & Dustin T. Duncan, *Health App Use Among US Mobile Phone Owners: A National Survey*, 3 JMIR mHealth & uHealth e101 at 5 (2015). Further research is being done on externally driven mobile interventions. An NIH study found that text messages are a useful way to help homeless veterans "reduce missed visits and emergency department use." D. Keith McInnes, et al., *Retaining Homeless Veterans in Outpatient Care: A Pilot Study of Mobile Phone Text Message Appointment Reminders*, 104 Am. J. Pub. Health S588, S593 (2014). Initial results on a pilot program called Text2Quit, in which educational and motivational text messages are sent to smokers who are trying to quit, showed high user engagement and support for further research. Lorien C. Abroms, et al., *Text2Quit: Results From a Pilot Test of a Personalized, Interactive Mobile Health Smoking Cessation Program*, 17 J. Health Comm. 44, 44 (2012).

---

[47] http://www.healthcareitnews.com/news/american-well-partners-samsung-electronics-mobile-telehealth.

G. Cell Phones Are Especially Critical to Vulnerable Populations.

As the internet becomes ever more essential to daily American life, some of the most vulnerable populations in the country are relying on cell phones for access. Pushed by economic necessity, the need to access critical government services or obtain medical or emergency information, cell phones are not optional for these populations. Deeming their use as a voluntary convenience risks amplifying the vulnerabilities they already face.

Overall, younger adults, lower-income Americans, and non-white Americans are particularly likely to own smartphones, but not have broadband in their homes. *Mobile Fact Sheet.* Smartphones are more popular among lower socioeconomic status groups because they are less expensive than laptops and come bundled with internet access. See Eric Tsetsi & Stephen A. Rains, *Smartphone Internet Access and Use: Extending the Digital Divide and Usage Gap*, 5 Mobile Media & Comm. __ (2017) (published online but not yet in print).[48] Pew found that in households making less than $30,000 per year, 21% of smartphone owners rely on their phones for internet access. *Mobile Fact Sheet*, and Mary Madden and others found that "63% of smartphone Internet users who live in households earning less than $20,000 per year say they mostly go online using their cell phone." Mary Madden, et al., *Privacy, Poverty and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 Wash. U. L. Rev. 53, 70 (2017).

---

[48] http://journals.sagepub.com/doi/abs/10.1177/2050157917708329.

Many of the cell phone use cases discussed above have disparate effects on different populations. For example, African Americans "tend to rely heavily on smartphones" when looking for work. *Searching for Work* at 17. Thirty-eight percent of African-Americans seek jobs on their smartphones, while only 24% of white people do. *Id.* Given that Pew's data was collected in 2014, and Pew found a sharp uptick in smartphone ownership in lower income and over-50 populations last year, *Mobile Fact Sheet*, these estimates almost surely undercount.

Mobile access is helping people that would not otherwise use banks. Seven percent of U.S. households are unbanked and another 20% are considered "underbanked," which means the household has a checking or savings account, but still used "products or services from an alternative financial services provider in the past 12 months," such as check cashing or payday loans. *FDIC Study* at 13. Underbanked households are more likely than banked to need to pay someone—a landlord, for example—the same day they receive funds. The "convenience and speed" of mobile banking gives them the ability to use traditional banks more often rather than alternative, often predatory, financial services. Penny Crosman, *Banks Experiment with Apps for the Underbanked*, American Banker (Sept. 22, 2014).[49]

Mobile services are especially critical for the ill and disabled, as well. For people with disabilities, cell phones are used as assistive technologies. Numerous scholars have illustrated the importance

---

[49] https://www.americanbanker.com/news/banks-experiment-with-apps-for-the-underbanked.

of mobile devices to children with hearing, speech, and cognitive disabilities. See, *e.g.*, Meryl Alper, Giving Voice: Mobile Communication, Disability, and Inequality (2017); Gerard Goggin & Christopher Newell, *Disabling Cell Phones*, The Cell Phone Reader: Essays in Social Transformation 155 (2007). For example, "Smartphones . . . can be a primary or vital form of communication for children who have difficulty or prefer not to use embodied oral speech." Meryl Alper, Digital Youth with Disabilities 24 (2014). And as discussed above, cell phones are necessary for chronically ill patients to maintain contact with physicians and loved ones to manage their conditions, *Health Benefits and Barriers to Cell Phone Use*, at 243, and nearly all HIV-positive people in a recent study viewed a cell phone as a primary necessity. *Cell Phone Disconnection Disrupts Access*, at 1429.

In sum, cell phones are particularly necessary tools for people who are disadvantaged in society. A finding that the Fourth Amendment does not protect CSLI will disproportionately impact these vulnerable populations.

H. United States Government Programs and Initiatives Have Recognized the Necessity of Mobile Technology.

In the present case, the Government argues that Carpenter's CSLI was voluntarily given to his phone carrier. But the U.S. Government has elsewhere acknowledged the necessity of cell phones to daily life by recognizing that government services must be optimized for mobile use.

Under the Obama administration, the Digital Government Initiative set a goal to "enable the American people and an increasingly mobile workforce to access high-quality digital government information and services anywhere, anytime, on any device." White House, Digital Government.[50] In addition, the Obama administration also deeply subsidized cell phone services for households below 135% of the poverty line or who are participating in another federal assistance program. Universal Service Administration, *Do I Qualify?*[51] Comparing the most recent available data from both this program and unemployment insurance, in 23 states, a greater percentage of eligible people took advantage of the cell phone subsidies than unemployment benefits. Julia Ticona, *In 23 States, Lifeline Participation Higher Than Unemployment Insurance* (Aug. 8, 2017).[52]

In May 2017, the Connect to Government Act was introduced in the House to require federal agencies to optimize their websites for mobile users. The author of the act, Representative Robin Kelly, said "In 2017, it's unreasonable that one in 10 Americans cannot connect with their government because they only use mobile devices . . . No business or organization would build a website without mobile optimization, why should the government?" Press Release, *Congresswoman Kelly Leads Effort to Move*

---

[50] https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html.

[51] http://www.lifelinesupport.org/ls/do-i-qualify/default.aspx.

[52] http://juliaticona.com/lifeline-participation.

Government Websites Into the 21st Century, Website of Congresswoman Robin Kelly (May 9, 2017).[53]

Other parts of the government have implicitly recognized the importance of cell phones by investing heavily in mobile app interfaces. The Department of Agriculture recently invested $1.5 million to develop an app to help people apply for food stamps in New York City, where 68% of people who receive them have smartphones. Nikita Stewart, *Applying for Food Stamps in New York? There's an App for That*, N.Y. Times (July 24, 2017).[54] In 2012, the Social Security Administration created a Digital Strategy Plan, which emphasized the need to create mobile apps for wage reporting, optimization of FAQs, contacts with SSA offices, and financial planning. Social Security Administration, *Digital Government Strategy*.[55] In addition, U.S. Citizenship and Immigration Services has made numerous smartphone-driven changes after finding that nearly 30% of visitors to the English site and over 50% of those visiting the Spanish site use a mobile device. USCIS, *USCIS Website, E-Verify Now Optimized for Mobile Devices* (Feb. 29, 2016).[56]

These heavy government investments in mobile happened because cell phones are ubiquitous and important to those people that rely on government programs. Because these efforts are

---

[53] https://robinkelly.house.gov/media-center/press-releases/congresswoman-kelly-leads-effort-to-move-government-websites-into-the.

[54] https://www.nytimes.com/2017/07/24/nyregion/food-stamps-hra-app.html.

[55] https://www.ssa.gov/digitalstrategy.

[56] https://www.uscis.gov/news/uscis-website-e-verify-now-optimized-mobile-devices.

increasingly optimized for mobile engagement, the technology will only become more indispensable for engaging with the government in the future.

CONCLUSION

Ninety-five percent of Americans have cell phones because cell phones have become an essential part of daily life. To hold that CSLI is transmitted voluntarily for purposes of the third-party doctrine would be to find that nearly all Americans have waived their Fourth Amendment protections in data transmitted by those devices. That rule would fall even harder on the most vulnerable in society, who rely on cell phones more than others.

We urge the Court to limit the third-party doctrine and construe it as inapplicable to cell phone location data.

Respectfully Submitted,

MARCIA HOFMANN
KENDRA ALBERT
ZEITGEIST LAW PC
25 Taylor St.
San Francisco, CA 94102

ANDREW D. SELBST
Counsel of Record
DATA & SOCIETY
RESEARCH INSTITUTE
36 W. 20th St.
11th Floor
New York, NY 10011
(617) 504-1982
andrew@datasociety.net

Dated: August 11, 2017

Government Websites Into the 21st Century, Website of Congresswoman Robin Kelly (May 9, 2017).[53]

Other parts of the government have implicitly recognized the importance of cell phones by investing heavily in mobile app interfaces. The Department of Agriculture recently invested $1.5 million to develop an app to help people apply for food stamps in New York City, where 68% of people who receive them have smartphones. Nikita Stewart, *Applying for Food Stamps in New York? There's an App for That*, N.Y. Times (July 24, 2017).[54] In 2012, the Social Security Administration created a Digital Strategy Plan, which emphasized the need to create mobile apps for wage reporting, optimization of FAQs, contacts with SSA offices, and financial planning. Social Security Administration, *Digital Government Strategy*.[55] In addition, U.S. Citizenship and Immigration Services has made numerous smartphone-driven changes after finding that nearly 30% of visitors to the English site and over 50% of those visiting the Spanish site use a mobile device. USCIS, *USCIS Website, E-Verify Now Optimized for Mobile Devices* (Feb. 29, 2016).[56]

These heavy government investments in mobile happened because cell phones are ubiquitous and important to those people that rely on government programs. Because these efforts are

---

[53] https://robinkelly.house.gov/media-center/press-releases/congresswoman-kelly-leads-effort-to-move-government-websites-into-the.

[54] https://www.nytimes.com/2017/07/24/nyregion/food-stamps-hra-app.html.

[55] https://www.ssa.gov/digitalstrategy.

[56] https://www.uscis.gov/news/uscis-website-e-verify-now-optimized-mobile-devices.

increasingly optimized for mobile engagement, the technology will only become more indispensable for engaging with the government in the future.

CONCLUSION

Ninety-five percent of Americans have cell phones because cell phones have become an essential part of daily life. To hold that CSLI is transmitted voluntarily for purposes of the third-party doctrine would be to find that nearly all Americans have waived their Fourth Amendment protections in data transmitted by those devices. That rule would fall even harder on the most vulnerable in society, who rely on cell phones more than others.

We urge the Court to limit the third-party doctrine and construe it as inapplicable to cell phone location data.

Respectfully Submitted,

MARCIA HOFMANN
KENDRA ALBERT
ZEITGEIST LAW PC
25 Taylor St.
San Francisco, CA 94102

ANDREW D. SELBST
Counsel of Record
DATA & SOCIETY
RESEARCH INSTITUTE
36 W. 20th St.
11th Floor
New York, NY 10011
(617) 504-1982
andrew@datasociety.net

Dated: August 11, 2017

39

No. 16-402

Supreme Court, U.S.
FILED
AUG 14 2017
OFFICE OF THE CLERK

IN THE

Supreme Court of the United States

RECORD AND BRIEFS

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, BRENNAN CENTER FOR JUSTICE, THE CONSTITUTION PROJECT, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS AND NATIONAL ASSOCIATION OF FEDERAL DEFENDERS IN SUPPORT OF PETITIONER

ANDREW CROCKER
Counsel of Record
JENNIFER LYNCH
JAMIE WILLIAMS
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
andrew@eff.org

Counsel for Amici Curiae

(Additional Counsel listed inside cover)

274756

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

Library of Congress
Law Library

FAIZA PATEL
MICHAEL W. PRICE
RACHEL LEVINSON-WALDMAN
BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
161 Avenue of the Americas,
12th Floor
New York, NY 10013

Counsel for Brennan Center for Justice at NYU School of Law

JAKE LAPERRUQUE
THE CONSTITUTION PROJECT
1200 18th Street NW,
Suite 1000
Washington, DC 20036

Counsel for The Constitution Project

DAVID OSCAR MARKUS
Co-Chair, Amicus Committee
NATIONAL ASSOCIATION
OF CRIMINAL DEFENSE
LAWYERS
40 NW Third Street, PH1
Miami, FL 33128

Counsel for National Association of Criminal Defense Lawyers

MEGHAN SKELTON
DONNA COLTHARP
SARAH GANNETT
DAN KAPLAN
Co-Chairs, NAFD Amicus Committee
NATIONAL ASSOCIATION OF
FEDERAL DEFENDERS
850 West Adams Street,
Suite 201
Phoenix, AZ 85007

Counsel for National Association of Federal Defenders

TABLE OF CONTENTS

Page

TABLE OF CONTENTS i

TABLE OF CITED AUTHORITIES iii

STATEMENT OF INTEREST 1

INTRODUCTION AND SUMMARY OF THE ARGUMENT 1

ARGUMENT 3

I. There Has Been a Dramatic Increase in Location Data Generated by Cell Phones, Collected by Third Parties, and Routinely Obtained by Law Enforcement Without a Warrant 5

A. The Number of Cell Phones and Cell Sites Has Increased Significantly in the Last Thirty Years 5

B. As the Number of Cell Towers and Amount of Data Transmitted Increases, the Location Data Generated by Cell Phones Becomes Increasingly More Detailed 10

C. Law Enforcement Routinely Requests Access to Months of CSLI Without a Warrant 13

Table of Contents

Page

II. CSLI Paints a Revealing Portrait of a Person's Movements, Presenting Even Greater Privacy Concerns Than the GPS Tracker at Issue in *Jones*. 15

III. The Third-Party Doctrine Is "Ill-Suited to the Digital Age" and Should Not Apply to CSLI. 19

A. Cell Phone Users Do Not "Voluntarily Convey" CSLI to Service Providers. 20

i. The Vast Majority of CSLI Is Generated Automatically 20

ii. There Is No Reasonable Alternative to Conveying CSLI to Third-Party Service Providers 22

B. The Third-Party Doctrine Is Incompatible with Modern Communications, and Americans Reasonably Expect Location Data to Remain Private. 23

C. Cell Phone Location Information Implicates First Amendment Interests that Require Fourth Amendment Protection. 26

CONCLUSION 30

APPENDIX 1a

TABLE OF CITED AUTHORITIES

Page

CASES

Bond v. United States,
529 U.S. 334 (2000) 25

City of Ontario v. Quon,
560 U.S. 746 (2010) 22

Commonwealth v. Augustine,
4 N.E.3d 846 (Mass. 2014) 18, 21

Ferguson v. City of Charleston,
532 U.S. 67 (2001) 25

In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.,
396 F. Supp. 2d 747 (S.D. Tex. 2005) 15

In re Application for Tel. Info. Needed for a Criminal Investigation,
119 F. Supp. 3d 1011 (N.D. Cal. 2015) . . . . . *passim*

In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.,
809 F. Supp. 2d 113 (E.D.N.Y. 2011) 17

In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't,
620 F.3d 304 (3d Cir. 2010) 21

Cited Authorities

Page

In re Application of U.S. for Historical Cell Site Data,
724 F.3d 600 (5th Cir. 2013).....11

Katz v. United States,
389 U.S. 347 (1967).....20

Kyllo v. United States,
533 U.S. 27 (2001).....18, 26

Marcus v. Search Warrants of Prop. at 104 E. Tenth St.,
367 U.S. 717 (1961).....26

Maryland v. Macon,
472 U.S. 463 (1985).....27

NAACP v. Alabama,
357 U.S. 449 (1958).....18

New York. v. P. J. Video,
475 U.S. 868 (1986).....27

Oliver v. United States,
466 U.S. 170 (1984).....25-26

People v. Weaver,
909 N.E.2d 1195 (N.Y. 2009).....29

Riley v. California,
134 S. Ct. 2473 (2014)..... *passim*

Cited Authorities

Page

Roaden v. Kentucky,
413 U.S. 496 (1973) 27, 29

Roberts v. U.S. Jaycees,
468 U.S. 609 (1984) 18

Smith v. Maryland,
442 U.S. 735 (1979) ..... *passim*

Stanford v. Texas,
379 U.S. 476 (1965) 26-27, 29

State v. Earls,
70 A.3d 630 (N.J. 2013) 22

Stoner v. California,
376 U.S. 483 (1963) 25

Tracey v. State,
152 So. 3d 504 (Fla. 2014) 11, 16, 21

United States v. Carpenter,
819 F.3d 880 (6th Cir. 2016) ..... *passim*

United States v. Cooper,
No. 13–cr–00693–SI–1, 2015 WL 881578
(N.D. Cal. March 2, 2015) 22

United States v. Cotterman,
709 F.3d 952 (9th Cir. 2013) 28

Page

United States v. Davis,
785 F.3d 498 (11th Cir. 2015) 11, 17, 21

United States v. Graham,
824 F.3d 421 (4th Cir. 2016) ..... *passim*

United States v. Jacobsen,
466 U.S. 109 (1984) 27

United States v. Jones,
565 U.S. 400 (2012) ..... *passim*

United States v. Miller,
425 U.S. 435 (1976) 19, 25

United States v. Stimler,
Nos. 15-4053, 15-4094, 15-4095,
2017 WL 3080866 (3d Cir. July 7, 2017) 21

Walter v. United States,
447 U.S. 649 (1980) 27

Zurcher v. Stanford Daily,
436 U.S. 547 (1978) 27, 29

STATUTES

18 U.S.C. §§ 2701–2712 5

Cited Authorities

Page

CONSTITUTIONAL PROVISIONS

U.S. Const. amend. I ..... *passim*

U.S. Const. amend. IV ..... *passim*

LEGISLATIVE AUTHORITIES

Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance, Hearing Before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations, of the H. Comm. on the Judiciary, 113th Cong. 50 (2013) (written testimony of Professor Matt Blaze, University of Pennsylvania) 7, 9, 12, 13

OTHER AUTHORITIES

Monica Anderson, *6 Facts About Americans and Their Smartphones*, Pew Research Center (Apr. 1, 2015) 8

Apple, *Share Your Location With Your Family*.....23

AT&T, *AT&T Transparency Report* (Jan. 2016).....13

AT&T, *AT&T Transparency Report* (Feb. 2017) 13

Cited Authorities

Page

Kevin Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, 123 Yale L.J. Online 335 (2014) 16

Jan Lauren Boyles, et al., *Privacy and Data Management on Mobile Devices*, Pew Research Internet & Am. Life Project (2012).....24

CTIA—The Wireless Association, *Annual Year-End 2015 Top-Line Survey Results* (May 2016).....6, 8

CTIA—The Wireless Association, *Annual Year-End 2016 Top-Line Survey Results* (May 2017)..5, 7, 9, 10

David Deasy, *TRUSTe Study Reveals Smartphone Users More Concerned About Mobile Privacy Than Brand or Screen Size*, TRUSTe Blog (Sept. 5, 2013).....25

Jesus Diaz, *How Large Is a Petabyte?*, Gizmodo (July 8, 2009).....10

Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681 (2011).....11

Harris Interactive, *2013 Mobile Consumer Habits Study* (June 2013) 5

Page

Letter from Timothy P. McKone, Executive Vice President, AT&T, to Rep. Edward J. Markey (Oct. 3, 2013) 11

Mary Madden, et al., *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Ctr. (2014) 24

Pew Research Center, *Mobile Fact Sheet* (Jan. 12, 2017) 5, 8

Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, J. Nat'l Security L. & Pol'y (2015) 29

Marguerite Reardon, *Cell Phone Industry Celebrates Its 25th Birthday*, CNET (Oct. 13, 2008) 5

Bennett Stein, *Fighting a Striking Case of Warrantless Cell Phone Tracking*, ACLU (July 1, 2013) 17

T-Mobile, *T-Mobile Transparency Report for 2015* 14

Abigail Tracy, *T-Mobile Leads US Wireless Carriers In Government Data Requests*, Forbes (July 6, 2015) 14

Twitter, *FAQs About Adding Location to Your Tweets* 23

Cited Authorities

Page

U.S. Census Bureau, *U.S. and World Population Clock* 6

Verizon, *Verizon's Transparency Report for the First Half of 2015* (2015) 14

Verizon, *Verizon's Transparency Report for the Second Half of 2015* (2016) 14

Verizon, *Verizon's Transparency Report for the First Half of 2016: U.S. Report* (2016).....14

Verizon, *Verizon's Transparency Report for the Second Half of 2016: U.S. Report* (2017) 14

Verizon, *Verizon United States Report* (2016).....15

Kathryn Zickuhr, *Location-Based Services*, Pew Research Internet and American Life Project (Sept. 12, 2013) 24

STATEMENT OF INTEREST[1]

Amici are organizations committed to ensuring that constitutional rights are protected as technology advances and include the Electronic Frontier Foundation, Brennan Center for Justice, the Constitution Project, National Association of Criminal Defense Lawyers, and National Association of Federal Defenders. All of these organizations have appeared previously as *amici* before this Court. Their individual organizational statements are contained in the Appendix following this brief.

INTRODUCTION AND SUMMARY OF THE ARGUMENT

Cell phones have become "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014). In *Riley*, this Court recognized that the ubiquity of cell phones, combined with their capacity to hold vast quantities of detailed personal information—potentially the "sum of an individual's private life"—makes cell phones so qualitatively and quantitatively different from their analog counterparts as to require a warrant prior to search. *Id.* at 2489.

---

1. The parties' letters consenting to the filing of all *amicus* briefs have been filed with the Clerk's office. Pursuant to Supreme Court Rule 37.6, *amici* state that this brief was not authored in whole or in part by counsel for any party, and that no person or entity other than *amici* or their counsel made a monetary contribution to fund the preparation or filing of this brief. This brief does not purport to represent the position of NYU School of Law.

However, the private information available from cell phones is not limited to the data stored on the phone itself. For a phone to receive and share much of that data—to be usable at all—it must connect with a cell tower. Every time it does, it generates information, stored by the phone company, about which tower the phone connected to—essentially where the phone was—on a given date and time. These small bits of data—called cell site location information (CSLI)—are aggregated by providers and, like GPS data, they "generate[] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

CSLI is proving increasingly useful to law enforcement. As cell phone use has increased, so too has the number of cell towers or cell "sites," leading to increasingly precise location information on individuals. Equipped with CSLI, police can now not only place suspects at specific crime scenes, but can also reconstruct almost anyone's movements for many months in the past. Yet law enforcement obtains this type of information without a warrant, tens of thousands of times a year.

This case requires the Court to address whether the Fourth Amendment prohibits the warrantless seizure and search of CSLI.[2] The Sixth Circuit below relied on this Court's opinion in *Smith v. Maryland*, 442 U.S. 735 (1979), to hold Americans lack a reasonable expectation

---

2. The issues in this case are highly similar to *United States v. Graham*, 824 F.3d 421 (4th Cir. 2016), which remains pending on a petition for certiorari in this Court. *See* No. 16-6308.

of privacy in CSLI because it is a business record held by third-party service providers. *United States v. Carpenter*, 819 F.3d 880, 887 (6th Cir. 2016).

But *Smith* cannot govern here. The now-routine use of CSLI to reconstruct individuals' movements over extended periods of time was "nearly inconceivable just a few decades ago," *Riley*, 134 S. Ct. at 2484. Whatever wisdom the so-called third-party doctrine had in 1979 when *Smith* was decided, it is entirely "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 565 U.S. at 417 (Sotomayor, J. concurring). The Court should instead hold that CSLI is subject to the full protection of the Fourth Amendment.

ARGUMENT[3]

Americans carry their cell phones with them everywhere and, as they do, they automatically generate granular and detailed information about where they have been, and when. The amount of sensitive location data generated by cell phones has increased dramatically in recent years, matched only by the increase in warrantless law enforcement demands for it. But if the Fourth Amendment is to have any force in the digital age, then it must keep up with how Americans use cell phone technology. Using CSLI to determine individuals' movements is as revealing as the GPS tracking this Court found problematic in *Jones*, if not more so. And because

3. All websites cited in this brief were last visited on August 8, 2017.

CSLI is becoming more precise over time, it can rival GPS tracking in geographical accuracy.

Applying the third-party doctrine to CSLI is inconsistent with the original reasoning underlying this Court's third-party doctrine cases. These cases stand for the proposition that individuals lose their expectation of privacy in certain records they "voluntarily" convey to third parties. But CSLI is purely a byproduct of owning and carrying an operational phone—it is automatically created whenever the phone tries to send and receive information, generally without forethought or conscious action by the owner. And cell phones are so essential to modern life that it is practically impossible to avoid creating CSLI in the first place. As a result, individuals do not "voluntarily" convey this information to cellular providers in any normal sense of the word. Instead, Americans overwhelmingly consider location privacy important and many take steps to limit sharing of their location.

Finally, CSLI implicates the same kind of expressive and associational activities that the Framers sought to safeguard in the Fourth Amendment. They specified that "papers" are protected against unreasonable searches and seizures to ensure that the warrant requirement applied in full force when these rights were at stake—as in this case. This Court should recognize the First Amendment functions that cell phones play in the digital age and grant CSLI the Fourth Amendment's full protection.

I. There Has Been a Dramatic Increase in Location Data Generated by Cell Phones, Collected by Third Parties, and Routinely Obtained by Law Enforcement Without a Warrant.

A. The Number of Cell Phones and Cell Sites Has Increased Significantly in the Last Thirty Years.

Owning a cell phone is not a luxury; at least 95% of all American adults have a cell phone, and most carry their phone with them everywhere they go.[4] As the Court explained in *Riley*, the "element of pervasiveness that characterizes cell phones" has a crucial impact on the Fourth Amendment issues here. *Riley*, 134 S. Ct. at 2490.

The first commercial cell phone service was offered in the United States in 1983[5]—four years after this Court's seminal decision in *Smith v. Maryland* and three years before Congress enacted the Stored Communications Act ("SCA"), 18 U.S.C. §§2701–2712. Since that time, the number of mobile device accounts in the United States has grown to an estimated 396 million—72 million more accounts than people at the end of 2016.[6]

---

4. *See Mobile Fact Sheet*, Pew Research Center (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile; *2013 Mobile Consumer Habits Study* 2–3, Harris Interactive (June 2013), http://pages.jumio.com/rs/jumio/images/Jumio%20-%20Mobile%20Consumer%20Habits%20Study-2.pdf.

5. Marguerite Reardon, *Cell Phone Industry Celebrates Its 25th Birthday*, CNET (Oct. 13, 2008), https://www.cnet.com/news/cell-phone-industry-celebrates-its-25th-birthday.

6. CTIA—The Wireless Association, *Annual Year-End 2016 Top-Line Survey Results* 3 (May 2017) ("CTIA 2016 Survey"),

CSLI is becoming more precise over time, it can rival GPS tracking in geographical accuracy.

Applying the third-party doctrine to CSLI is inconsistent with the original reasoning underlying this Court's third-party doctrine cases. These cases stand for the proposition that individuals lose their expectation of privacy in certain records they "voluntarily" convey to third parties. But CSLI is purely a byproduct of owning and carrying an operational phone—it is automatically created whenever the phone tries to send and receive information, generally without forethought or conscious action by the owner. And cell phones are so essential to modern life that it is practically impossible to avoid creating CSLI in the first place. As a result, individuals do not "voluntarily" convey this information to cellular providers in any normal sense of the word. Instead, Americans overwhelmingly consider location privacy important and many take steps to limit sharing of their location.

Finally, CSLI implicates the same kind of expressive and associational activities that the Framers sought to safeguard in the Fourth Amendment. They specified that "papers" are protected against unreasonable searches and seizures to ensure that the warrant requirement applied in full force when these rights were at stake—as in this case. This Court should recognize the First Amendment functions that cell phones play in the digital age and grant CSLI the Fourth Amendment's full protection.

I. There Has Been a Dramatic Increase in Location Data Generated by Cell Phones, Collected by Third Parties, and Routinely Obtained by Law Enforcement Without a Warrant.

A. The Number of Cell Phones and Cell Sites Has Increased Significantly in the Last Thirty Years.

Owning a cell phone is not a luxury; at least 95% of all American adults have a cell phone, and most carry their phone with them everywhere they go.[4] As the Court explained in *Riley*, the "element of pervasiveness that characterizes cell phones" has a crucial impact on the Fourth Amendment issues here. *Riley*, 134 S. Ct. at 2490.

The first commercial cell phone service was offered in the United States in 1983[5]—four years after this Court's seminal decision in *Smith v. Maryland* and three years before Congress enacted the Stored Communications Act ("SCA"), 18 U.S.C. §§2701–2712. Since that time, the number of mobile device accounts in the United States has grown to an estimated 396 million—72 million more accounts than people at the end of 2016.[6]

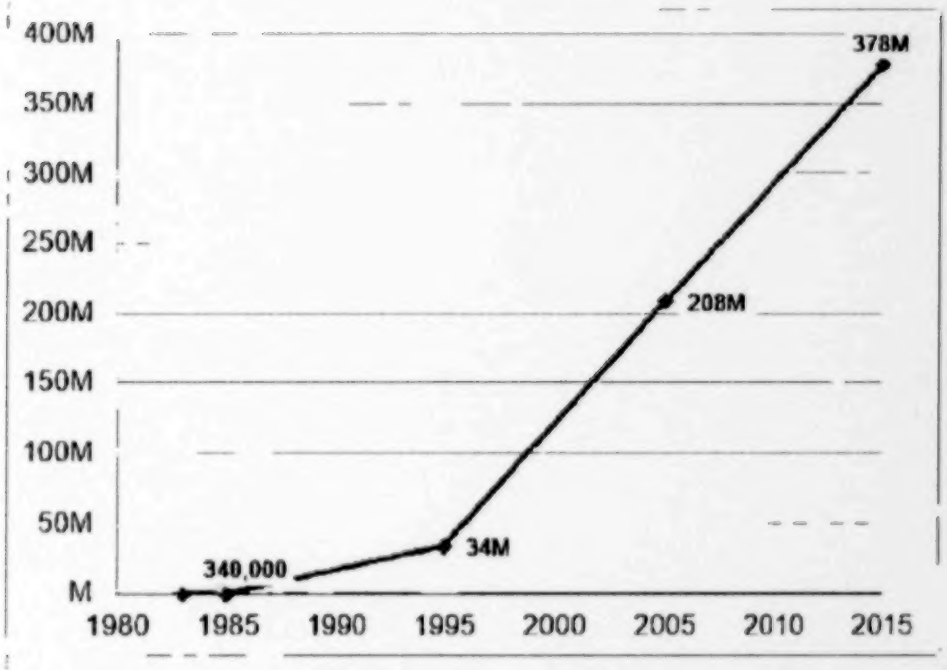
---

4. *See Mobile Fact Sheet*, Pew Research Center (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile; *2013 Mobile Consumer Habits Study* 2–3, Harris Interactive (June 2013), http://pages.jumio.com/rs/jumio/images/Jumio%20-%20Mobile%20Consumer%20Habits%20Study-2.pdf.

5. Marguerite Reardon, *Cell Phone Industry Celebrates Its 25th Birthday*, CNET (Oct. 13, 2008), https://www.cnet.com/news/cell-phone-industry-celebrates-its-25th-birthday.

6. CTIA—The Wireless Association, *Annual Year-End 2016 Top-Line Survey Results* 3 (May 2017) ("CTIA 2016 Survey"),

Chart 1: Number of Mobile Device Subscriptions in United States[7]



Cell phones send and receive radio signals via base stations, known as cell towers. Towers typically have multiple cell "sites" facing in three or four different

---

https://www.ctia.org/docs/default-source/default-document-library/annual-year-end-2016-top-line-survey-results-final.pdf (396 million "wireless subscriber connections"); *see* U.S. Census Bureau, *U.S. and World Population Clock*, http://www.census.gov/popclock (estimated U.S. population 324 million on December 31, 2016).

7. Charts 1–3 were generated using statistics from an annual survey of wireless service providers conducted by CTIA—The Wireless Association, the leading wireless industry trade association. *See* CTIA—The Wireless Association, *Annual Year-End 2015 Top-Line Survey Results* 3 (May 2016) ("CTIA 2015 Survey"), *available at* http://bit.ly/2h38cS4.

directions, each containing antennae that detect radio signals emanating from phones and that connect the phones to the cellular network.[8] Cell phones automatically try to connect to the nearest or strongest base station, and, as users move farther away from one base station and closer to another, their phones automatically transfer the connection to the new base station.

As cell phone use has increased, service providers have installed more cell sites to handle the load.[9] There are at least 300,000 cell sites operating in the United States,[10] and these sites include many more antennae constantly communicating with all phones in range.[11]

---

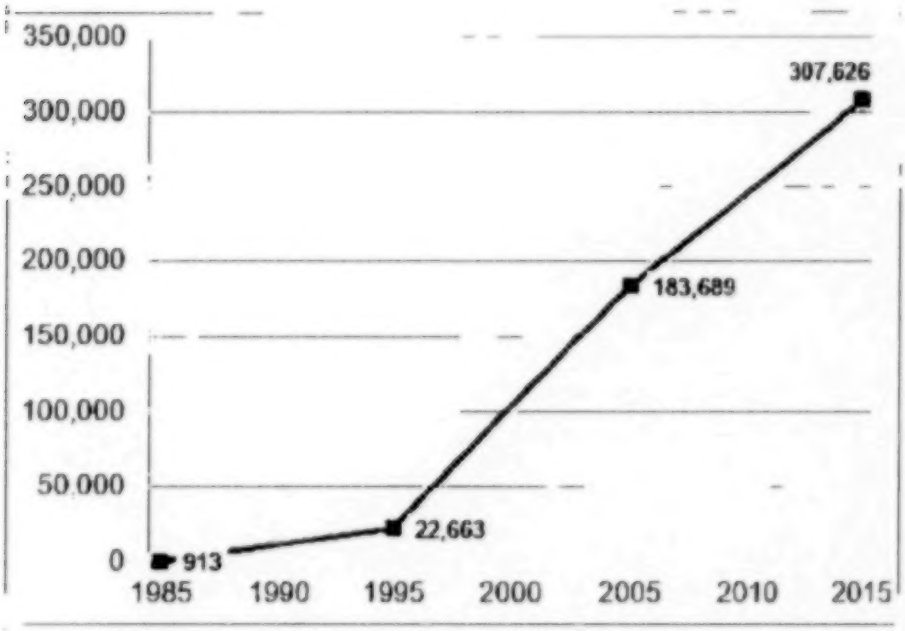
8. *See* Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance, Hearing Before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations, of the H. Comm. on the Judiciary, 113th Cong. 50, at 6, 9 (2013) (written testimony of Professor Matt Blaze, University of Pennsylvania) ("2013 Blaze Testimony"), *available at* https://judiciary.house.gov/wp-content/uploads/2016/02/Blaze-Testimony.pdf.

9. 2013 Blaze Testimony at 10 ("A sector base station can handle only a limited number of simultaneous call connections given the amount of radio spectrum 'bandwidth' allocated to the wireless carrier.").

10. CTIA 2016 Survey at 4 (308,334 cell sites in 2016).

11. A different estimate reports 645,891 towers and 1,892,359 antennae—including those used for cellular and other communications services—as of July 9, 2017. AntennaSearch.com, http://antennasearch.com.

Chart 2: Number of Cell Sites in United States[12]



Modern cell phones' increasing sophistication and improved capabilities have also driven the need for more cell sites. After Apple released the iPhone in 2007, "smartphones" took off in popularity. Now more than 77% of Americans own smartphones.[13] For a significant percentage of "smartphone-dependent" Americans, their phones are their only means of accessing the Internet; this is disproportionately true for young adults, people of color, and lower-income Americans.[14]

---

12. CTIA 2015 Survey at 10.

13. *Mobile Fact Sheet*, Pew Research Center; CTIA 2016 Survey at 2 (262 million smartphones in use in 2016).

14. Monica Anderson, *6 Facts About Americans and Their Smartphones*, Pew Research Center (Apr. 1, 2015), http://www.pewresearch.org/fact-tank/2015/04/01/6-facts-about-americans-

Smartphones allow users to do everything from take and share photos, connect with friends through a variety of video and text-based communication tools, find the fastest route to a new location, stream music, research health information, play games, and track finances—and do all of these things at the same time. As a result, smartphones transmit and receive vast amounts of data. As more Americans have switched to smartphones, the amount of data transferred over wireless networks has increased significantly—3,500% between 2010 and 2016 alone[15]—and service providers have installed more towers to handle that increase.[16]

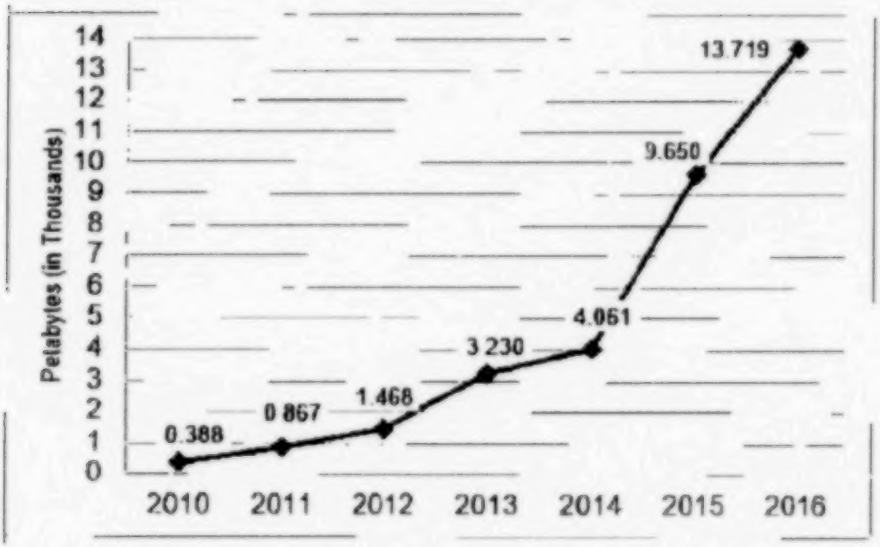
---

and-their-smartphones (noting the following percentages of "smartphone-dependent" Americans: 18-29 year olds (15%); adults with an annual household income of less than $30,000 (13%) versus adults with an income of $75,000 or above (1%); Latinos (13%) and African Americans (12%) versus whites (4%)).

15. CTIA 2016 Survey at 3 (388 billion megabytes in 2010, 13,719 billion megabytes in 2016).

16. 2013 Blaze Testimony at 11.

Chart 3: Wireless Data Traffic (in Petabytes)[17]



B. As the Number of Cell Towers and Amount of Data Transmitted Increases, the Location Data Generated by Cell Phones Becomes Increasingly More Detailed.

When cell phones connect to cell sites, they generate CSLI—a record of the location of the cell tower the phone connected to at a specific moment in time. Modern cell phones—particularly smartphones—generate vast amounts of CSLI because they routinely send and receive data whenever the phone is on.

---

17. CTIA 2016 Survey at 4. One source has described a petabyte of data as the equivalent of 20 million four-drawer filing cabinets filled with text. *See* Jesus Diaz, *How Large Is a Petabyte?*, Gizmodo (July 8, 2009), http://gizmodo.com/5309889/how-large-is-a-petabyte.

Cell phones generate CSLI even in the absence of any user interaction with the phone, in part due to "applications that continually run in the background, sending and receiving data" (*e.g.*, email applications) "without a user having to interact with the cellular telephone." *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011, 1014 (N.D. Cal. 2015) ("*2015 N.D. Cal. Opinion*") (quoting Declaration of FBI Special Agent Hector M. Luna). Although some courts have limited their analysis of CSLI to data generated when users place and terminate a call,[18] the government has admitted that it seeks access to CSLI generated by apps running in the background. *See id.* at 1033.

Cell phones connect with towers to exchange data on average every seven to nine minutes but can attempt to connect as frequently as every seven seconds.[19] Because these data exchanges create a record of when the user connected to the tower, along with the location of the tower itself, they reveal where the phone—and by proxy, its owner—has traveled. Cell providers store this data for up to five years[20] and can also track CSLI in near real-time.[21]

---

18. *See United States v. Davis*, 785 F.3d 498, 503 (11th Cir. 2015); *see also In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600, 615 (5th Cir. 2013) ("Fifth Circuit Opinion").

19. *2015 N.D. Cal. Opinion*, 119 F. Supp. 3d at 1028; Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681, 703 (2011).

20. *See Letter from Timothy P. McKone, Executive Vice President, AT&T, to Rep. Edward J. Markey* 3 (Oct. 3, 2013), *available at* http://www.markey.senate.gov/imo/media/doc/2013-10-03_ATT_re_Carrier.pdf.

21. *See Tracey v. State*, 152 So. 3d 504, 507 (Fla. 2014).

Law enforcement officers rely on CSLI to place a suspect at a specific location at a specific time, such as at the scene of a crime. *See, e.g.*, *United States v. Carpenter*, 819 F.3d 880, 884 (6th Cir. 2016) (FBI used CSLI to place defendants to within 1/2 to 2 miles of robbery locations at times robberies occurred); *see also United States v. Graham*, 796 F.3d 332, 341 (4th Cir. 2015) *vacated by* 824 F.3d 421 (4th Cir. 2016) (en banc). In the past, CSLI was less accurate, because it consisted only of the location of the base station the phone connected to and the approximate "sector" served by that base station. Sectors could be several miles in diameter, so the phone could theoretically be anywhere within that area.

Now, however, CSLI has become much more detailed and specific. As the number of cell towers has increased and cell sites have become more concentrated, the geographic area covered by each cell sector has shrunk.[22] Cell phone triangulation (data from three towers instead of one) allows more precise location tracking. With newer cell technology, providers can determine not just the location of the cell site the phone connects to, but, by "correlating the precise time and angle at which a given device's signal arrives at multiple sector base stations," they can determine where the phone is located within a sector.[23] This can shrink accuracy down to within 50 meters.[24] Providers are also using small base stations designed to serve individual homes or offices, or even

22. 2013 Blaze Testimony at 10.

23. *Id.* at 12.

24. *Id.*

particular floors of buildings.[25] With these technologies, providers can determine "a phone's latitude and longitude at a level of accuracy that can approach that of GPS."[26]

These advances in cell service technology have especially impacted dense metropolitan areas with large numbers of mobile devices attempting to exchange data. In these areas, the higher concentration of towers and antennae allow phones' locations to be pinpointed with even greater accuracy.[27]

C. Law Enforcement Routinely Requests Access to Months of CSLI Without a Warrant.

As cell phones saturate the country, law enforcement agencies routinely seek access to CSLI in criminal cases. The number of these requests is staggering. For example, AT&T alone received 70,528 requests for CSLI in 2016 and 76,340 requests in 2015.[28] Verizon received 53,532

---

25. *Id.* at 11.

26. *Id.* at 12.

27. *Id.* at 10-12.

28. *See* AT&T, *AT&T Transparency Report* 4, 8 (Feb. 2017), http://about.att.com/content/dam/csr/Transparency%20Reports/Feb-2017-Transparency-Report.pdf; AT&T, *AT&T Transparency Report* 4 (Jan. 2016), http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_Transparency%20Report_Jan%202016.pdf (disclosing number of requests for historical CSLI, real-time CSLI, and "cell tower dumps" identifying information for all phones that connected to a tower during a given period of time).

Law enforcement officers rely on CSLI to place a suspect at a specific location at a specific time, such as at the scene of a crime. *See, e.g.*, *United States v. Carpenter*, 819 F.3d 880, 884 (6th Cir. 2016) (FBI used CSLI to place defendants to within 1/2 to 2 miles of robbery locations at times robberies occurred); *see also United States v. Graham*, 796 F.3d 332, 341 (4th Cir. 2015) *vacated by* 824 F.3d 421 (4th Cir. 2016) (en banc). In the past, CSLI was less accurate, because it consisted only of the location of the base station the phone connected to and the approximate "sector" served by that base station. Sectors could be several miles in diameter, so the phone could theoretically be anywhere within that area.

Now, however, CSLI has become much more detailed and specific. As the number of cell towers has increased and cell sites have become more concentrated, the geographic area covered by each cell sector has shrunk.[22] Cell phone triangulation (data from three towers instead of one) allows more precise location tracking. With newer cell technology, providers can determine not just the location of the cell site the phone connects to, but, by "correlating the precise time and angle at which a given device's signal arrives at multiple sector base stations," they can determine where the phone is located within a sector.[23] This can shrink accuracy down to within 50 meters.[24] Providers are also using small base stations designed to serve individual homes or offices, or even

22. 2013 Blaze Testimony at 10.

23. *Id.* at 12.

24. *Id.*

particular floors of buildings.[25] With these technologies, providers can determine "a phone's latitude and longitude at a level of accuracy that can approach that of GPS."[26]

These advances in cell service technology have especially impacted dense metropolitan areas with large numbers of mobile devices attempting to exchange data. In these areas, the higher concentration of towers and antennae allow phones' locations to be pinpointed with even greater accuracy.[27]

C. Law Enforcement Routinely Requests Access to Months of CSLI Without a Warrant.

As cell phones saturate the country, law enforcement agencies routinely seek access to CSLI in criminal cases. The number of these requests is staggering. For example, AT&T alone received 70,528 requests for CSLI in 2016 and 76,340 requests in 2015.[28] Verizon received 53,532

---

25. *Id.* at 11.

26. *Id.* at 12.

27. *Id.* at 10-12.

28. *See* AT&T, *AT&T Transparency Report* 4, 8 (Feb. 2017), http://about.att.com/content/dam/csr/Transparency%20Reports/Feb-2017-Transparency-Report.pdf; AT&T, *AT&T Transparency Report* 4 (Jan. 2016), http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_Transparency%20Report_Jan%202016.pdf (disclosing number of requests for historical CSLI, real-time CSLI, and "cell tower dumps" identifying information for all phones that connected to a tower during a given period of time).

requests in 2016 and 50,066 requests in 2015.[29] T-Mobile, the parent company of MetroPCS and the service provider in this case, *Carpenter*, 819 F.3d at 885, does not report requests for CSLI specifically, but the company received far more requests for customer data as a whole than its much larger rivals.[30]

As high as these numbers are, they do not tell the full story. Each request may seek information on many different phones. For example, in this case, officers relied on three requests to access information about 16 different phones. *Carpenter*, 819 F.3d at 884. The quantity of data requested for each phone may vary, although a

---

29. *See* Verizon, *Verizon's Transparency Report for the Second Half of 2016: U.S. Report* (2017), http://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2017/01/Transparency-Report-US-2H-2016.pdf; Verizon, *Verizon's Transparency Report for the First Half of 2016: U.S. Report* (2016), https://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2016/07/Transparency-Report-US-1H-2016.pdf; Verizon, *Verizon's Transparency Report for the Second Half of 2015* (2016), https://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2016/07/Transparency-Report-US-2H-2015.pdf; Verizon, *Verizon's Transparency Report for the First Half of 2015* (2015), https://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2016/01/Verizon-Transparency-Report-2015-first-half.pdf (numbers include "location information" and cell tower dumps).

30. Abigail Tracy, *T-Mobile Leads US Wireless Carriers In Government Data Requests*, Forbes (July 6, 2015), http://www.forbes.com/sites/abigailtracy/2015/07/06/t-mobile-leads-u-s-wireless-carriers-in-government-data-requests/#5cb644f54c88; T-Mobile, *T-Mobile Transparency Report for 2015, available at* https://newsroom.t-mobile.com/content/1020/files/2015TransparencyReport.pdf.

single request often produces CSLI that covers very long periods. Here, the FBI obtained three to four months of data, 819 F.3d at 895 (Stranch, J., concurring), while in *Graham*, agents were able to obtain 221 days of location information for Mr. Graham and his co-defendant with a single request. 796 F.3d at 341 (panel opinion).

The majority of these demands for CSLI are warrantless. In 2016, Verizon reported that up to three-quarters of all law enforcement requests for historical and real-time location information were made via a court order rather than warrant,[31] like the orders issued under 18 U.S.C. § 2703(d) that the government obtained in both this case and *Graham*. *Carpenter*, 819 F.3d at 884; *Graham*, 796 F.3d at 344 (panel).

II. CSLI Paints a Revealing Portrait of a Person's Movements, Presenting Even Greater Privacy Concerns Than the GPS Tracker at Issue in *Jones*.

The amount of CSLI generated as a result of society's reliance on cell phones means that law enforcement has access to an incredibly detailed picture of people's private lives and associations. *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). As noted in one of the first published opinions to address CSLI, the "combination of market and regulatory stimuli ensures that cell phone tracking will become more precise with each passing year." *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 755 (S.D. Tex. 2005).

---

31. *See* Verizon, *Verizon United States Report* (2016), https://www.verizon.com/about/portal/transparency-report/?page_id=2133.

Until the twenty-first century, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." *Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment). But CSLI has eviscerated that expectation and presents even greater privacy concerns than the GPS device this Court considered in *Jones*.[32]

First, a GPS device attached to a car can only go where the car goes, while a cell phone goes everywhere its owner goes. As this Court noted in *Riley*, "three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting they even use their phones in the shower." 134 S. Ct. at 2490 (citations omitted). Therefore, unlike GPS monitoring of a vehicle, examination of historical CSLI over an extended period as in this case cannot be confined to public spaces and "will invariably enter constitutionally protected areas, such as private residences." *2015 N.D. Cal. Opinion*, 119 F. Supp. 3d at 1023; *Tracey*, 152 So. 3d at 524 (real time "cell phone tracking can easily invade the right to privacy in one's home or other private areas, a matter that the government cannot always anticipate and one which, when it occurs,

---

32. According to one estimate, covert car pursuit can cost $275 per hour while location tracking via a cell phone can cost as little as $0.04 per hour, meaning that CSLI has increased government's capacity to track individuals by a factor of thousands. *See* Kevin Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, 123 Yale L.J. Online 335 (2014), http://yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones.

is clearly a Fourth Amendment violation."). And, in fact, using records about a defendant in *Graham*, the ACLU was able to infer details about his patterns of movement and presence in private spaces, including when he and his pregnant wife visited her obstetrician, when he traveled to or from his home, and nights spent away from home.[33]

Second, CSLI can give law enforcement far more information about a person's movements than the 28 days of monitoring that five members of this Court found problematic in *Jones*. *See* 565 U.S. at 430 (Alito, J., concurring in the judgment) (line at which tracking of vehicle became a search "was surely crossed before the 4-week mark"); *id.* at 413 (Sotomayor, J., concurring). Here, the government obtained 88 days and 127 days worth of location information from each defendant respectively. In other cases, the government has sought similarly extended periods of records, up to seven months of location information worth in a single request. *Davis*, 785 F.3d at 501 (67 days); *In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 114 (E.D.N.Y. 2011) (113 days); *United States v. Jones*, 908 F. Supp. 2d 203, 206 (D.D.C. 2012) (180 days); *Graham*, 796 F.3d at 349 (221 days). Because cell providers keep records of CSLI for up to five years, law enforcement officers could seek access to this data for even longer periods of time. Such extensive monitoring reveals a wealth of information about a person's expressive and associational activities protected by the First Amendment

33. *See* Bennett Stein, *Fighting a Striking Case of Warrantless Cell Phone Tracking*, ACLU (July 1, 2013), https://www.aclu.org/blog/fighting-striking-case-warrantless-cell-phone-tracking (noting records were analyzed with Mr. Graham's "assistance and permission").

in addition to the Fourth Amendment's protections against unreasonable searches. *See Smith*, 442 U.S. at 751 (Marshall, J. dissenting) (citing *NAACP v. Alabama*, 357 U.S. 449, 463 (1958)); *Roberts v. U.S. Jaycees*, 468 U.S. 609, 617-18 (1984).

Third, historical CSLI allows police to reconstruct a person's *past* movements. As Justice Alito noted in *Jones*, tracking a car's location for 28 days "would have [traditionally] required a large team of agents, multiple vehicles, and perhaps aerial assistance." 565 U.S. at 429 (Alito, J., concurring in the judgment). But CSLI allows police to go back in time to recreate a person's past movements, something not possible with the GPS tracker in *Jones* and *never* available through traditional law enforcement investigative techniques. *See Commonwealth v. Augustine*, 4 N.E.3d 846, 865 (Mass. 2014).

Finally, CSLI is generated for *all* phones, not simply those under investigation. Accordingly, unlike the GPS device in *Jones*, police need not even know in advance whether they want to track a particular individual. Rather, they have the ability to track nearly *any* person's location.

This Court has noted that it is "foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001). With historical CSLI, the "practical" privacy protections of tracking a person's movement for months in the "pre-computer age"—namely difficulty and cost—have faded away. *Jones*, 565 U.S. at 429 (Alito, J., concurring in the judgment).

III. The Third-Party Doctrine Is "Ill-Suited to the Digital Age" and Should Not Apply to CSLI.

The majority opinion in *Carpenter* relied on this Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979) (citing *United States v. Miller*, 425 U.S. 435, 442 (1976)), to hold that the Fourth Amendment does not protect CSLI. *Smith* is the principal basis for the so-called third-party doctrine, which the government argues denies Fourth Amendment protection for some information that is "voluntarily" conveyed to "third parties." But as Justice Sotomayor suggested in *United States v. Jones*, the third-party doctrine is "ill suited to the digital age" and should not now be extended to modern communications data like CSLI. 565 U.S. at 417 (Sotomayor, J., concurring).

First, disclosing CSLI to a service provider is not "voluntary" in any realistic sense of the word. Cell phones create CSLI constantly and automatically, even when they are not in active use. Moreover, they have become essential to daily life, and are crucial vehicles for First Amendment activity. Requiring Americans to forgo their phones in exchange for privacy would therefore present an untenable choice that is inconsistent with the history and purpose of the Fourth Amendment.

Second, the third-party doctrine is at odds with the way technology works and how people communicate today. Relying on *Smith*, some courts have mistakenly viewed information as either completely secret or presumptively public, failing to account for more nuanced understandings of privacy.

Finally, the third-party doctrine rests on outdated expectations about the "assumption of risk" involved in

making a phone call that fail to account for the modern First and Fourth Amendment implications of data like CSLI. Communications data should command heightened constitutional protections, and at minimum, a warrant requirement.

A. Cell Phone Users Do Not "Voluntarily Convey" CSLI to Service Providers.

In *Katz*, the Court pointed out that individuals could exercise their right to privacy in a public phone booth by remembering to close the phone booth door, thereby taking an affirmative step to exclude the "uninvited ear." *Katz v. United States*, 389 U.S. 347, 352 (1967). But for cell phone users, there is no door, no possible way to protect the privacy of personal data like CSLI. Exposing one's location to service providers through CSLI is an inescapable part of having a cell phone. There is no practical alternative, no option to mask the metadata,[34] no way to close the proverbial phone booth door. *See Katz*, 389 U.S at 352.

i. The Vast Majority of CSLI Is Generated Automatically.

It is a Fourth Amendment fiction that individuals "voluntarily" convey CSLI as one would dial a phone number. Users do not intentionally create CSLI and

---

34. Many smartphones include a location privacy setting that, when enabled, prevents applications from accessing the phone's location. However, this setting has no impact on a carrier's ability to learn the cell sector in use, thus giving phone users a false sense of privacy. *2015 N.D. Cal. Opinion*, 119 F. Supp. 3d at 1025.

have no real choice in the matter. In fact, it is "unlikely that cell phone customers are [even] aware that their cell phone providers collect and store historical location information." *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 317 (3d Cir. 2010); *see also United States v. Stimler*, Nos. 15-4053, 15-4094, 15-4095, 2017 WL 3080866, at *5 (3d Cir. July 7, 2017) (users do not voluntarily disclose CSLI to service providers); *Augustine*, 4 N.E.3d at 862 (same).

Rather, as described above, phones generate CSLI whenever they are on and searching for a signal—frequently, automatically, and regardless of whether the device is actively in use. CSLI includes data generated when users make calls, but that is a drop in the bucket compared to the data "generated by *passive* activities such as automatic pinging, continuously running applications ('apps'), and the receipt of calls and text messages." *2015 N.D. Cal. Opinion*, 119 F. Supp. 3d at 1024 (internal quotations and citation omitted). Further, the amount of data produced by such "passive" activities dwarfs the number of records from actually making phone calls, and is created "with far less intent, awareness, or affirmative conduct on the part of the user than what was at issue in . . . *Smith*." *Id.* at 1029. Such unwitting generation of CSLI does not amount to a "voluntary conveyance" under the third-party doctrine. *Id.*; *see also Davis*, 785 F.3d at 534 (Martin, J., dissenting); *Tracey*, 152 So.3d at 525-26.

ii. There Is No Reasonable Alternative to Conveying CSLI to Third-Party Service Providers.

The only way to avoid producing a comprehensive record of one's movements and associations based on CSLI is to stop carrying a cell phone, as some courts have suggested. *See, e.g., Carpenter,* 819 F.3d at 888; *Graham*, 824 F.3d at 427-28. But if a cell phone can be considered a "feature of human anatomy," then owning and carrying one is hardly a choice at all. *Riley*, 134 S. Ct. at 2484. Given that nearly all American adults own a cell phone, the position that cell phone users volunteer their location information simply by choosing to activate and use their phones and to carry the devices is untenable and unrealistic. *See State v. Earls*, 70 A.3d 630, 641 (N.J. 2013).

Furthermore, as this Court has repeatedly recognized, cell phones have become essential to the exercise of First Amendment freedoms. Indeed, they are "so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010); *Riley*, 134 S. Ct. at 2484; *see also United States v. Cooper*, No. 13–cr–00693–SI–1, 2015 WL 881578, at *8 (N.D. Cal. March 2, 2015) (cell phones are "ubiquitous, and for many, an indispensable gizmo to navigate the social, economic, cultural and professional realms of modern society."). Privacy cannot be the price of exercising those First Amendment freedoms.

B. The Third-Party Doctrine Is Incompatible with Modern Communications, and Americans Reasonably Expect Location Data to Remain Private.

The third-party doctrine is an exceedingly blunt instrument. In its strongest formulation, it divides the world in half: data is either completely secret or it is not private at all. But in practice, the privacy of communications metadata like CSLI is not an all-or-nothing endeavor. Some people may affirmatively choose to disclose their location information publicly, as when "geotagging" a Tweet.[35] On the other hand, people may restrict affirmative sharing of their location information to a more limited audience, like family or close friends.[36] And at other times, users may not consciously opt to share their location with anyone at all. But even the decision to "turn off" location sharing has no effect on the ability of service providers to know where a subscriber's phone is, assuming it is working and connected to their network. *2015 N.D. Cal. Opinion*, 119 F. Supp. 3d at 1025. If the third-party doctrine were to apply in this context, then the whereabouts of every cell phone user in America would never be private for Fourth Amendment purposes, no matter which other human beings—if any—they actually shared that information with.

---

35. *See* Twitter, *FAQs About Adding Location to Your Tweets*, https://support.twitter.com/articles/78525.

36. *See* Apple, *Share Your Location With Your Family*, https://support.apple.com/en-us/HT201087 (describing how Apple users can share their iPhone location with family members, with select family members, or no one at all).

In fact, recent studies show that Americans generally expect their location information to remain private, even though they may at times share it with others. In 2014, the Pew Research Center reported that 82% of Americans consider the details of their physical location over time to be sensitive information—more sensitive than their relationship history, religious or political views, or the content of their text messages.[37] In 2012, another Pew study found that cell phone owners take steps to protect their personal information and mobile data, and more than half of smartphone owners have uninstalled or decided to not install an app due to privacy concerns.[38] Additionally, more than 30% of smartphone owners polled took affirmative steps to safeguard their privacy and 19% turned off location tracking on their phones (which disables location tracking for certain apps but does not prevent the service provider from logging CSLI).[39] The numbers are higher for teenagers, with nearly half of all teenagers turning location services off.[40] A 2013 survey conducted on behalf of Internet company TRUSTe found

---

37. Mary Madden, et al., *Public Perceptions of Privacy and Security in the Post-Snowden Era* 34, 36–37, Pew Research Ctr. (2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf (50% of respondents believed location information was "very sensitive.").

38. Jan Lauren Boyles, et al., *Privacy and Data Management on Mobile Devices*, Pew Research Internet & Am. Life Project (2012), http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices.

39. *Id.*

40. Kathryn Zickuhr, *Location-Based Services*, Pew Research Internet and American Life Project (Sept. 12, 2013), http://www.pewinternet.org/2013/09/12/location-based-services/.

69% of American smartphone users were concerned about being tracked.[41]

Correspondingly, the Court should decline to adopt a blanket rule that CSLI lacks Fourth Amendment protection simply because it is shared with a third party. Indeed, the Court's decisions in *Smith* and *Miller* should not be read to endorse open-ended application of the third party doctrine in this way. The Court has repeatedly found that the Fourth Amendment protects some types of personal information, even if it is exposed to a third-party. *See, e.g., Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (patient has reasonable expectation of privacy in diagnostic test results held by hospital); *see also Bond v. United States*, 529 U.S. 334, 338–39 (2000) (passenger retained expectation of privacy in luggage placed in bus overhead bin despite possibility of external inspection by others); *Stoner v. California*, 376 U.S. 483, 489-90 (1963) (hotel guests are entitled to constitutional protection even though they provide "implied or express permission" for third parties to access their rooms). Communications data, like CSLI, should receive at least as much constitutional protection, even if individuals "voluntarily" convey it through third-party service providers.

In this light, applying the third-party doctrine to CSLI would defy Americans' expectations about privacy and disregard the decisions they actually make about what information to share. *Cf. Oliver v. United States*,

---

41. David Deasy, *TRUSTe Study Reveals Smartphone Users More Concerned About Mobile Privacy Than Brand or Screen Size*, TRUSTe Blog (Sept. 5, 2013), http://www.truste.com/blog/2013/09/05/truste-study-reveals-smartphone-users-more-concerned-about-mobile-privacy-than-brand-or-screen-size.

466 U.S. 170, 178 (1984) (noting that one factor the Court uses to assess "the degree to which a search infringes upon individual privacy" is the "societal understanding that certain areas deserve the most scrupulous protection from government invasion"). It would also allow for the warrantless tracking of the historical movements of anyone who carries a cell phone—nearly the entire population of the country.

Fortunately, the Court made clear in *Smith* itself that a "normative inquiry" would be necessary if individuals were not accorded a reasonable expectation of privacy consistent with "well-recognized Fourth Amendment freedoms." 442 U.S. at 740 n.5. In other words, the Fourth Amendment must protect CSLI to put limits on the "power of technology to shrink the realm of guaranteed privacy." *Kyllo*, 533 U.S. at 34.

C. Cell Phone Location Information Implicates First Amendment Interests that Require Fourth Amendment Protection.

Cell phone location information implicates the kind of expressive and associational activities that the Fourth Amendment was designed to protect. By giving "papers" equal billing with "persons," "houses," and "effects," the Framers indicated that courts have a special obligation to safeguard First Amendment information from unreasonable searches and seizures. *See* U.S. Const. amend. IV; *Marcus v. Search Warrants of Prop. at 104 E. Tenth St.*, 367 U.S. 717, 729 (1961) ("The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."); *Stanford*

v. Texas, 379 U.S. 476, 482 (1965) (describing the history of the Fourth Amendment as "largely a history of conflict between the Crown and the press").

Accordingly, courts should apply the Fourth Amendment's warrant requirement with "scrupulous exactitude" when significant First Amendment rights are at stake. *Stanford*, 379 U.S. at 485; *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978); *see also New York. v. P. J. Video*, 475 U.S. 868, 873-75 (1986) (films); *Maryland v. Macon*, 472 U.S. 463, 468 (1985) (magazines); *United States v. Jacobsen*, 466 U.S. 109, 114 (1984) (letters); *Walter v. United States*, 447 U.S. 649, 655 (1980) (books). A search or seizure that endangers First Amendment interests must, at the least, be made pursuant to a warrant supported by probable cause. *See Zurcher*, 436 U.S. at 565; *Roaden v. Kentucky*, 413 U.S. 496, 504 (1973) (requiring a warrant to seize an allegedly obscene film because "[t]he setting of the bookstore or the commercial theater ... invokes such Fourth Amendment warrant requirements").

In *Riley*, the Court reinforced this approach by requiring a warrant for cell phone searches incident to arrest because "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated" by most physical searches. 134 S. Ct. at 2488-89. Significantly, the unanimous Court was alarmed that a warrantless search would yield not only text messages and emails, but also *"[h]istoric location information"* that "can reconstruct someone's movements down to the minute, not only around town but also within a particular building." 134 S. Ct. at 2490 (emphasis added). Citing Justice Sotomayor's concurrence in *Jones*, the Court determined that such information is qualitatively different

from physical records (like those in *Smith*, perhaps) because such a "comprehensive record of a person's public movements . . . reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* (citing *Jones*, 565 U.S. at 415).

The common denominator in these decisions is that the data implicates the protected expressive and associational information the Framers sought to shield from warrantless government interference. Of course, the phone records in *Smith* involved private communications as well. 442 U.S. at 742. But comparing phone records in 1979 to communications metadata in 2017 is like "saying a ride on horseback is materially indistinguishable from a flight to the moon." *See Riley*, 134 S. Ct. at 2488; *see also United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013) (distinguishing the search of a laptop from the search of hand luggage because "technology matters").

Not only is the creation of CSLI unavoidable, but it is also simple to infer otherwise private expressive and associational activities from it in ways that were highly unlikely in *Smith*. This recognition again undercuts the "voluntariness" rationale at the heart of the third-party doctrine. Phone users in 1979 may have "assumed the risk" that the numbers they dial could be divulged to police, *Smith*, 442 U.S. at 745, but they did not assume they would be disclosing their religion, political affiliation, or sexual preferences—and neither did the Justices.

Even in limited quantities, these staccato signals can be a telltale sign of social, political, and religious activities. As in the GPS-tracking context, CSLI can reveal other activities of "indisputably private nature,"

like a visit to the "psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (quoting *People v. Weaver*, 909 N.E.2d 1195, 1999 (N.Y. 2009)).

The third-party doctrine advanced in *Smith* may have been appropriate for phone calls in 1979, but it is a poor match for the digital age. Communications data, like CSLI, has such significant First Amendment implications that it demands Fourth Amendment protection. *See Roaden*, 413 U.S. at 504 (the Court should examine Fourth Amendment reasonableness "in the light of the values of freedom of expression"); *Stanford*, 379 U.S. at 485; *Zurcher*, 436 U.S. at 564; *see also* Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. Nat'l Security L. & Pol'y, 270-71 (2015). CSLI implicates the same kind of expressive and associational activities that the Framers sought to protect by including "papers" in the text of the Fourth Amendment, and this Court should guard it accordingly. *See Riley*, 134 S. Ct. at 2491 (Fourth Amendment requires "clear guidance to law enforcement through categorical rules").

CONCLUSION

For the reasons stated above, this Court should hold that sensitive records like cell site location information are protected by the Fourth Amendment's warrant requirement.

Dated: August 14, 2017

Respectfully submitted,

FAIZA PATEL
MICHAEL W. PRICE
RACHEL LEVINSON-WALDMAN
BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
161 Avenue of the Americas,
12th Floor
New York, NY 10013

Counsel for Brennan Center for Justice at NYU School of Law

ANDREW CROCKER
Counsel of Record
JENNIFER LYNCH
JAMIE WILLIAMS
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
andrew@eff.org

Counsel for Amici Curiae

JAKE LAPERRUQUE
THE CONSTITUTION PROJECT
1200 18th Street NW,
Suite 1000
Washington, DC 20036

Counsel for The Constitution Project

DAVID OSCAR MARKUS
Co-Chair, Amicus Committee
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
40 NW Third Street, PH1
Miami, FL 33128

Counsel for National Association of Criminal Defense Lawyers

MEGHAN SKELTON
DONNA COLTHARP
SARAH GANNETT
DAN KAPLAN
Co-Chairs, NAFD Amicus Committee
NATIONAL ASSOCIATION OF FEDERAL DEFENDERS
850 West Adams Street,
Suite 201
Phoenix, AZ 85007

Counsel for National Association of Federal Defenders

APPENDIX

APPENDIX

The Electronic Frontier Foundation ("EFF") is a nonprofit, member-supported civil liberties organization working to protect rights in the digital world. EFF actively encourages and challenges government and the courts to support privacy and safeguard individual autonomy as emerging technologies become prevalent in society. EFF has served as *amicus* in Fourth Amendment cases before this Court, including in *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015), *Riley v. California*, 134 S. Ct. 2473 (2014), *Maryland v. King*, 133 S. Ct. 1958 (2013), *United States v. Jones*, 565 U.S. 400 (2012), and *City of Ontario v. Quon*, 560 U.S. 746 (2010). EFF has also served as amicus in numerous cases addressing Fourth Amendment protections for CSLI, including, *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010); *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *Commonwealth v. Augustine*, 4 N.E.3d 846 (Mass. 2014); *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015); *In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011 (N.D. Cal. 2015); and *United States v. Graham*, 824 F.3d 421 (4th Cir. 2016).

The Brennan Center for Justice at NYU School of Law is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice. The Center's Liberty and National Security (LNS) Program uses innovative policy recommendations, litigation, and public advocacy to advance effective national security policies that respect the rule of law and constitutional values. The LNS Program is particularly concerned with domestic

intelligence gathering policies, including the dragnet collection of Americans' communications and personal data, and the concomitant effects on First and Fourth Amendment freedoms. As part of its work in this area, the Center has filed numerous *amicus* briefs on behalf of itself and others in cases involving electronic surveillance and privacy issues, including *Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 565 U.S. 400 (2012); *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *petition for cert. docketed*, No. 16-402 (Sept. 28, 2016); *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016), *petition for cert. docketed*, No. 16-263 (Aug. 30, 2016); *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 829 F.3d 197 (2d Cir. 2016), *petition for reh'g* en banc *filed*, No. 14-2985 (Oct. 17, 2016); *United States v. Moalin*, No. 13-50572 (9th Cir. filed Nov. 5 1015); and *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015).

The Constitution Project ("TCP") is a constitutional watchdog that brings together legal and policy experts from across the political spectrum to promote and defend constitutional safeguards. TCP's bipartisan Liberty and Security Committee, founded in the aftermath of September 11th, is composed of policy experts, legal scholars, and former high-ranking government officials from all three branches of government. This diverse group makes policy recommendations to protect both national security and civil liberties, for programs ranging from government surveillance to U.S. detention. Based upon their reports and recommendations, TCP files amicus briefs in litigation related to these issues. TCP is dedicated

to ensuring that transformative changes in technology do not undermine the privacy rights that the Framers enshrined in our Constitution. For example, TCP's Liberty and Security Committee has published reports on public video surveillance systems (analyzing how rapid technological advances have eroded the distinction between private and public spaces in the context of such systems) and location tracking (finding that the Fourth Amendment requires law enforcement to obtain a warrant before employing GPS technology to conduct prolonged tracking of an individual's movements, even if on public streets).

The National Association of Federal Defenders ("NAFD"), formed in 1995, is a nationwide, nonprofit, volunteer organization whose membership is comprised of attorneys who work for federal public and community defender organizations authorized under the Criminal Justice Act. Each year, federal defenders represent tens of thousands of individuals in federal court. *Amicus* NAFD therefore has both particular expertise and interest in the subject matter of this litigation.

The National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL was founded in 1958, and has a nationwide membership of many thousand direct members, and up to 40,000 members when affiliates are included. NACDL's members include private criminal defense lawyers, public defenders, military

defense counsel, law professors, and judges. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers. NACDL is dedicated to advancing the proper, efficient, and just administration of justice. Each year, NACDL files numerous briefs as *amicus curiae* in the United States Supreme Court and other federal and state courts, seeking to provide *amicus* assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole.

This case presents issues of great importance to NACDL and the clients its attorneys represent, including the rights embodied in the Fourth Amendment to be free from constant and pervasive governmental snooping into the most private of our affairs.

RECORD
AND
BRIEFS

Supreme Court, U.S.
FILED
AUG 14 2017
OFFICE OF THE CLERK

No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ of Certiorari to the
United States Court of Appeals for the Sixth Circuit

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND THIRTY-SIX TECHNICAL EXPERTS AND LEGAL SCHOLARS IN SUPPORT OF PETITIONER

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
JOHN DAVISSON
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

August 14, 2017

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

INTEREST OF THE *AMICI CURIAE* 1

SUMMARY OF THE ARGUMENT 6

ARGUMENT 7

I. The world has changed since *Smith v. Maryland*. The widespread use of mobile phones and the routine collection of detailed location data was not possible in 1979. 11

A. The analog phone system in the 1970s did not generate "out of band" personal data. ... 11

B. The pen register in *Smith* recorded only the outgoing numbers dialed by a single telephone customer. 14

C. Location data for telephone users did not exist in the 1970s. 17

D. The Court recognized in *Riley* that modern communications services store a wealth of sensitive personal data. 24

II. Cell phone users do not "assume the risk" that their personal data will be disclosed to others. 26

A. Cell phone users expect that their personal data will be kept private. 27

B. Cell phone users limit access to their location data 31

III. This Court must determine the appropriate scope of the Fourth Amendment. Then it is for Congress to develop an appropriate statutory framework. 35

CONCLUSION 40

TABLE OF AUTHORITIES

CASES

Arizona v. Evans,
514 U.S. 1 (1995) (O'Connor, J., concurring) 23

Berger v. New York,
388 U.S. 41 (1967) 36

In re iPhone Application Litigation,
6 F. Supp. 3d 1004 (N.D. Cal. 2013) 33

Katz v. United States,
389 U.S. 347 (1967) 36

Katz v. United States,
389 U.S. 347 (1967) (Harlan, J., concurring) 36

Kyllo v. United States,
533 U.S. 27 (2001) 23, 24

Marbury v. Madison,
5 U.S. 137 (1803) 39

Riley v. California,
134 S. Ct. 2473 (2014) 6, 7, 24, 25, 26, 36, 38

Smith v. Maryland,
442 U.S. 735 (1979) 2, 6, 14, 15, 22, 27

Smith v. Maryland,
442 U.S. 735 (1979) (Marshall, J., dissenting) . 9, 27

Smith v. Maryland,
442 U.S. 735 (1979) (Stewart, J., dissenting) 8

United States v. Barajas,
710 F.3d 1102 (10th Cir. 2013) 20, 22

United States v. Caplan,
255 F. Supp. 805 (E.D. Mich. 1966) 16

United States v. Denson,
775 F.3d 1214 (10th Cir. 2014) 24

United States v. Focarile,
340 F. Supp. 1033 (D. Md. 1972) 15, 16

United States v. Giordano,
416 U.S. 505 (1974) 15

United States v. Giordano,
416 U.S. 505 (1974) (Powell, J., dissenting)..... 15

United States v. Jones,
565 U.S. 400 (2012) 9

United States v. Jones,
565 U.S. 400 (2012) (Alito, J., concurring).... 7, 9, 35

United States v. Jones,
565 U.S. 400 (2012) (Sotomayor, J.,
concurring)..... 9

United States v. Miller,
425 U.S. 435 (1976) 26

United States v. N.Y. Tel. Co.,
434 U.S. 159 (1977) 14, 15

United States v. U.S. Dist. Court for Eastern Dist. of Mich.,
407 U.S. 297 (1972) 37

United States v. Wallace, __ F.3d ___,
2017 WL 3304087 (5th Cir. 2017)..... 20

STATUTES

47 U.S.C. § 222..... 22

Communications Assistance for Law Enforcement Act ("CALEA"), Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended at 47 U.S.C. §§ 1001–10) 10

47 U.S.C. § 1002(a)(2)(B) 10

Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801 *et seq.*) 37

50 U.S.C. § 1803 38

Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, Tit. III, 82 Stat. 197, 211–25 (codified as amended at 18 U.S.C. §§ 2510–20) 37

REGULATIONS

47 C.F.R. § 20.18 21

OTHER AUTHORITIES

A Guide to the Wireless Engineering Body of Knowledge (Andrzej Jajszcyk ed., 2d ed. 2011) 18

Alan Butler, *Get A Warrant: The Supreme Court's New Course for Digital Privacy Rights After* Riley v. California, 10 Duke J. Const. L. & Pub. Pol'y 83 (2014) 14

Alisdair Allan & Peter Warden, *Got an iPhone or 3G iPad? Apple is Recording Your Moves*, O'Reilly Radar (Apr. 20, 2011) 32

Anita L. Allen & Marc Rotenberg, *Privacy Law and Society* (3d ed. 2016) 9

Apple, *About Location Services and Privacy*, Apple Support (June 21, 2017) 31

Bruce Schneier, *Data and Goliath* (2015) 23

C.F. Ault, J.H. Brewster, T.S. Greenwood, R.E. Haglund, W.A. Read, & M.W. Rolund, *IA Processor: Memory Systems*, 56 Bell Sys. Tech. J. 181 (1977) 14

Caitlin D. Cottrill & Piyushimita "Vonu" Thakuriah, *Location Privacy Preferences: A Survey-based Analysis of Consumer Awareness, Trade-off and Decision-making*, 56 Transp. Res. Part C 132 (2015) 30

Dave McHoul, *Locating a 911 Caller*, Skyhook (June 2, 2016) 21, 22

David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 Minn. L. Rev. 62 (2013) 35

Eben Moglen, *The Tangled Web We Have Woven*, 56 Comms. ACM 20 (2013) 26

EPIC, *iPhones, iPads Collect and Store User Location Data* (Apr. 21, 2011) 32

Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 Mich. L. Rev. 485 (2013) 35

G.V. King, *Centralized Automatic Message Accounting System*, 33 Bell Sys. Tech. J. 1331 (1954) 12, 13

H.R. Rep. 103-821, pt. 1 (1994) 10

Hal Abelson, Hen Ledeen, & Harry Lewis, *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion* (2008) 25

Hannah Arendt, *The Origins of Totalitarianism* (1973) 20

Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1 (2008) 22

Jeffrey Rosen, *Protect Our Right to Anonymity*, N.Y. Times, Sept. 13, 2011, at A31 23

Kenneth Olmstead & Aaron Smith, *What the Public Knows About Cybersecurity*, PewResearch Center (Mar. 22, 2017) 29

Kenneth Olmstead, *A Third of Americans Live in a Household with Three or More Smartphones*, PewResearch Center (May 25, 2017) 28

Laura Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. Ann. Surv. Am. L. 553 (2017) 19

Lee Rainie, *The State of Privacy in Post-Snowden America*, PewResearch Center (Sept. 21, 2016) 29, 30

Letter from Sen. Al Franken to Steve Jobs, CEO of Apple (Apr. 20, 2011) 33

Marc Rotenberg & David Brody, *Protecting Privacy: The Role of the Courts and Congress*, Hum. Rts., March 2013 ..... 35, 36, 37

Matt Blaze, *How Law Enforcement Tracks Cellular Phones* (Dec. 13, 2013) 18

Michele Sequeira & Michael Westphal, *Cell Phone Science: What Happens When You Call and Why* (2010) 18, 19

Miguel Helft, *Jobs Said Apple Made Mistake with iPhone Data*, N.Y. Times, Apr. 27, 2011, at B3 33

Mobile Fact Sheet, PewResearch Center (Jan. 12, 2017) 28

Network Wiretapping Capabilities: Hearing Before the Subcomm. on Telecomm. & Fin. of the H. Comm. on Energy & Commerce, 103d Cong. (1994) (testimony of Hon. Louis J. Freeh, Director, Fed. Bureau of Investigation) 10

Phil Lapsley, *Exploding The Phone – Extras* (2013) 13

Press Release, Apple Q&A on Location Data (Apr. 27, 2011) 34

Press Release, Markey to Apple: Is It iPhone or iTrack? (April 21, 2011) 33

Robert Ellis Smith, *Location Location Location* (2014) 22

Robert G. Harris, *State Regulatory Policies and the Telecommunications/Information Infrastructure in The Changing Nature of Telecommunications/Information Infrastructure* (Computer Sci. & Telecomm. Bd. and Nat'l Research Council eds., 1995) 14

Robert J. Chapuis & Amos E. Joel, *100 Years of Telephone Switching, Part 2* (2003)..... 13

S. Rep. No. 90-1097 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112 37

S. Rep. No. 95-604, pt. 1 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3904 38

Samuel Alito et al., Final Report, *in Conference on the Boundaries of Privacy in American Society* (1972) 38

Statement for the Record from EPIC, Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services before the Subcomm. on the Constitution, Civil Rights, & Civil Liberties, of the House Comm. on Judiciary (June 24, 2010) 32

Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 26 Berkeley Tech. L.J. 117 (2012) 19

Stephen J. Blumberg & Julian V. Luke, Nat. Cent. for Health Statistics, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July–December 2016* (2017) 28

Washington Journal: Cell Phone Tracking and Privacy Issues (C-SPAN Apr. 26, 2011) 34

Wireless E911 Location Accuracy Requirements, *Fourth Report and Order*, 30 FCC Rcd 1259 (2015) 21

Wireless E911 Location Accuracy Requirements, *Third Further Notice of Proposed Rulemaking*, 29 FCC Rcd 2374 (2014) 21

Your Phone Dial Computes Your Bill, Popular Sci., Feb. 1949 12

INTEREST OF THE *AMICI CURIAE*

The Electronic Privacy Information Center (EPIC)[1] is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.

EPIC routinely participates as *amicus curiae* before this Court and other courts concerning privacy issues, new technologies, and constitutional interests. *See, e.g.*, *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017) (arguing that the First Amendment protects the right to access speech from the privacy of a personal electronic device); *Utah v. Streiff*, 136 S. Ct. 2056 (2016) (arguing that evidence obtained via suspicionless identification should be suppressed); *Riley v. California*, 134 S. Ct. 2473 (2014) (arguing that it is unreasonable to warrantlessly search a cell phone incident to an arrest); *Florida v. Harris*, 133 S. Ct. 1050 (2013) (arguing that the government bears the burden of establishing the reliability of new investigative techniques used in establishing probable cause for a search); *United States v. Jones*, 565 U.S. 400 (2012) (arguing that a warrant is required for the use of GPS tracking techniques); *State v. Earls*, 214 N.J.

---

[1] Both parties have filed letters of consent to the filing of all amicus briefs with the Clerk of the Court pursuant to Rule 37.3. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

564 (2013) (arguing that warrantless cell phone location tracking violates the Fourth Amendment); *Commonwealth v. Connolly*, 454 Mass. 808 (2009) (arguing that warrantless GPS tracking of a vehicle violates the Fourth Amendment).

EPIC seeks to preserve the Fourth Amendment and to prevent emerging technologies and new police practices from eroding constitutional privacy rights. This case presents a fundamental question about the scope of Fourth Amendment protections as applied to the collection of personal data—data that did not exist at the time the Court decided *Smith v. Maryland*, 442 U.S. 735 (1979). EPIC submits the following *amicus* brief, signed by distinguished technical experts and legal scholars, in support of the Fourth Amendment in the digital age.

Technical Experts and Legal Scholars

Ann M. Bartow
Director, Franklin Pierce Center for Intellectual Property and Professor of Law, University of New Hampshire School of Law

Colin J. Bennett
Professor, University of Victoria

Francesca Bignami
Professor of Law, The George Washington University Law School

David Chaum
Chaum, LLC

Danielle Keats Citron
Morton & Sophia Macht Professor of Law, University of Maryland School of Law

Julie Cohen
Mark Claster Mamolen Professor of Law and Technology, Georgetown Law

Jennifer Daskal
Associate Professor, American University Washington College of Law

Dr. Whitfield Diffie

Laura K. Donohue
Professor of Law, Director of The Center for National Security and the Law, Georgetown University Law Center

Cynthia Dwork
Distinguished Scientist, Microsoft Research

David J. Farber
Distinguished Career Professor of Computer Science and Public Policy, Carnegie Mellon University

Addison Fischer
Founder and Chairman, Fischer International Corp.

Hon. David Flaherty
Former Information and Privacy Commissioner for British Columbia

Deborah Hurley
Harvard University and Brown University

Ian Kerr
Canada Research Chair in Ethics, Law & Technology, University of Ottawa Faculty of Law

Chris Larsen
Executive Chairman, Ripple, Inc.

Harry R. Lewis
Gordon McKay Professor of Computer Science, Harvard University

Anna Lysyanskaya,
Professor of Computer Science, Brown University

Gary T. Marx
Professor Emeritus of Sociology, MIT

Mary Minow
Library Law Consultant

Erin Murphy
Professor of Law, NYU School of Law

Dr. Pablo Garcia Molina
Adjunct Professor, Georgetown University

Dr. Peter G. Neumann
Senior Principal Scientist, SRI International Computer Science Lab

Helen Nissenbaum
Professor, Cornell Tech Information Science, Professor, New York University (on leave), Media, Culture, and Communication & Computer Science

Dr. Deborah Peel, M.D.
Founder and Chair, Patient Privacy Rights

Ronald L. Rivest
Institute Professor of Electrical Engineering and Computer Science, MIT

Pamela Samuelson
Richard M. Sherman Distinguished Professor of Law and Information, University of California, Berkeley School of Law; Co-Director, Berkeley Center for Law & Technology

Bruce Schneier
Program Fellow, Harvard Kennedy School

Robert Ellis Smith
Publisher, Privacy Journal

Dr. Barbara Simons,
IBM Research (retired)

Nadine Strossen
John Marshall Harlan II Professor of Law, New York Law School; Former President, American Civil Liberties Union

Sherry Turkle,
Abby Rockefeller Mauzé Professor of the Social Studies of Science and Technology, MIT

Edward G. Viltz,
President and Chairman, Internet Collaboration Coalition

Jim Waldo
Gordon McKay Professor of the Practice of Computer Science, Chief Technology Officer, John A. Paulson School of Engineering and Applied Science, Professor of Technology Policy, Harvard Kennedy School

Christopher Wolf
Board Chair, Future of Privacy Forum

Shoshana Zuboff,
Charles Edward Wilson Professor of Business Administration, Emerita, Harvard Business School

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

Smith v. Maryland, 442 U.S. 735 (1979), arose in a world that no longer exists. In the 1970s, telephones were tethered to homes, offices, and street corners. Cell phones were not available, and logs of telephone customers' locations over the course of a day were neither recorded nor available for later inspection. Cell phones are now as necessary to the life of Americans as they are ubiquitous. They are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of the human anatomy." *Riley v. California*, 134 S. Ct. 2473, 2484 (2014). Yet, despite these fundamental changes, lower courts still apply Fourth Amendment concepts that were established when rotary phones sat on desk tops, the receivers connected with coiled wire.

This Court has never held that the government may search and seize records of where a person travels without triggering Fourth Amendment scrutiny. Indeed, the Court recently determined in *Riley* that the government could not seize such sensitive cell phone data without a warrant. There is also no evidence that cell phone users expect to be subject to such routine tracking of their private lives– quite the contrary. We as a society are not prepared to accept pervasive, warrantless location tracking as objectively reasonable.

The Court's decision in *Smith* does not determine the scope of Fourth Amendment protection today. In the modern era, cell phone location records provide a "comprehensive record of a person's public movements that reflects a wealth of detail about her

familial, political, professional, religious, and sexual associations." *Riley*, 134 S. Ct. at 2490 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)). And while Congress should address the "complex subject" of location tracking by enacting a "comprehensive statute," the Court bears the fundamental responsibility of determining the appropriate scope of the Fourth Amendment. *See Jones*, 565 U.S. at 427 (Alito, J., concurring); *see also* Edith J. Lapidus, *Eavesdropping on Trial* 1–26 (1974) (discussing the development of modern wiretap law, particularly the importance of the Court's decisions in *Berger* and *Katz* in the 1967 term that led to adoption of a comprehensive privacy law in 1968).

ARGUMENT

This case involves the warrantless collection of cell phone location records. In 1979, that data did not exist. Today, that data is maintained on all cell phone users in the United States. If the warrantless collection of location data is permissible in this case, then it would be permissible for every cell phone customer in the country.

In *Jones* (2012), this Court held unanimously that the warrantless tracking of a person's movement by means of a GPS attached to a vehicle was impermissible. Then the Court held in *Riley* (2014) that the traditional "search incident to arrest" exception did not apply to cell phones, given the wealth of personal data stored on the devices.

Despite the Court's recent rulings and the fundamental shift in communications technology that

has occurred since the 1970s, lower courts continue to follow *Smith* (1979) and hold that the Fourth Amendment does not apply to cell phone location data. These decisions are out of step with the current era. First, *Smith* is no longer applicable in the age of cell phones; modern call data bears little resemblance to the paper logs available in 1979. Second, cell phone users do not "assume the risk" that their personal data will be made available to any person at any time. Third, it is the Court and not Congress that should determine the appropriate scope of Fourth Amendment protections.

Even at the time that *Smith* was decided, the Court was closely divided over the appropriate degree of protection for pen register information. Justice Stewart was sharply critical of the Court's conclusion, noting that:

> I think that the numbers dialed from a private telephone--like the conversations that occur during a call--are within the constitutional protection recognized in *Katz*. It seems clear to me that information obtained by pen register surveillance of a private telephone is information in which the telephone subscriber has a legitimate expectation of privacy.

Smith, 442 U.S. at 747 (Stewart, J., dissenting). Justice Marshall also dissented, challenging the Court's "assumption of risk" analysis:

> [E]ven assuming, as I do not, that individuals 'typically know' that a phone company monitors calls for internal reasons, it does not follow that they expect this information to be made available to the public in general or the government in particular. Privacy is not a

> discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes . . . .

Smith, 442 U.S. at 749 (Marshall, J., dissenting).

Since *Smith* was decided in 1979, both the Court and Congress have recognized the need to limit warrantless location tracking. The Court unanimously rejected the government's argument in *Jones* that the attachment and use of a GPS device to track an individual's movements over several months was not a search under the Fourth Amendment. *Jones*, 565 U.S. 400. Five members of the Court agreed with Justice Alito's conclusion that "the lengthy monitoring that occurred . . . constituted a search under the Fourth Amendment." *Jones*, 565 U.S. at 431 (Alito, J., concurring); *see also Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) ("I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'"); Anita L. Allen & Marc Rotenberg, *Privacy Law and Society* 443 (3d ed. 2016) (explaining the view that "there were five votes [in *Jones*] for a *Katz*-based determination that GPS tracking violates the Fourth Amendment"). The Court's majority opinion in *Jones* also recognized that modern location tracking techniques make possible "dragnet-type law enforcement practices" that the Court explicitly refused to authorize in the 1980s beeper cases. *Jones*, 565 U.S. at 409 n.6 (quoting *United States v. Knotts*, 460 U.S. 276, 284 (1983)).

Congress has also recognized that special protections for location data are necessary to protect expectations of privacy. In 1994 Congress passed the Communications Assistance for Law Enforcement Act ("CALEA"), Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended at 47 U.S.C. §§ 1001–10), at the behest of then-FBI Director Louis Freeh. But even as Congress was significantly expanding law enforcement surveillance powers in CALEA, it explicitly prohibited the government from obtaining "any information that may disclose the physical location of the subscriber" when acting "solely pursuant to the authority for pen registers and trap and trace devices." 47 U.S.C. § 1002(a)(2)(B). Congress recognized that, at the time, "some cellular systems" generated "transactional data that could be obtained by a pen register [which] may include location information." H.R. Rep. No. 103-821, pt. 1, at 17 (1994). This limitation was proposed by the FBI as an assurance that the agency was not seeking a "pervasive, automated 'tracking' capability." *Network Wiretapping Capabilities: Hearing Before the Subcomm. on Telecomm. & Fin. of the H. Comm. on Energy & Commerce*, 103d Cong. 54 (1994) (testimony of Hon. Louis J. Freeh, Dir., Fed. Bureau of Investigation). Yet now the Government argues that the same location data it encouraged Congress to protect in 1994 should not be protected under the Fourth Amendment.

I. The world has changed since *Smith v. Maryland*. The widespread use of mobile phones and the routine collection of detailed location data was not possible in 1979.

The analog telephone network of the 1970s was entirely unlike today's digital network. In 1979, when *Smith* was decided, telephone service was provided as a public utility, local calls were not individually billed, and there was little transactional data generated by a private communication. It was only after the transition to "Signal System 7" ("SS7"), which followed *Smith*, that the challenge of collecting, storing, analyzing, safeguarding, and securing digital phone records emerged. In 1979, no one could have used call detail records to trace an individual's movements over time. A telephone number was tied to an address, not to an individual. Many phones were shared by multiple users in a home or office. In short, the records at issue in *Smith* revealed the numbers dialed, not a person's location. Today the communications network provides a vast range of voice, data, and messaging services and simultaneously records every transaction that occurs, tied directly to particular subscribers.

A. The analog phone system in the 1970s did not generate "out of band" personal data.

In the period leading up to the Court's decision in *Smith*, detailed phone records simply did not exist for local calls. Prior to the introduction of the earliest electronic switching systems in the 1960s and 1970s, the majority of telephone calls in the United States

were processed by analog switches that had limited accounting and billing capabilities. These analog switches relied on "Automatic Message Accounting" systems, which were introduced in the Bell System in 1948 and recorded customer data on perforated paper tapes (earlier systems relied on handwritten notes from telephone operators). G.V. King, *Centralized Automatic Message Accounting System*, 33 Bell Sys. Tech. J. 1331, 1332 (1954). These analog accounting systems were designed to handle three different types of calls: flat-rate local calls, message rate calls, and long distance toll calls. *Your Phone Dial Computes Your Bill*, Popular Sci., Feb. 1949, at 135–36. Most local calls were billed on a flat-rate monthly basis, and automated accounting equipment was not used to record any details about these calls. King, *supra*, at 1333. For calls billed on a message rate basis, the accounting system would record a two-line entry containing "the calling office code and telephone number, the billing index and the trunk identity," along with the duration of the call. *Id.* at 1339. The more extensive four-line entries also contained "the called office code and telephone number" but were only used for detail-billed toll calls and special bulk billed calls that required additional records. *Id.* In situations where a toll call could not be completed by a switch capable of automated message accounting, customers had to be connected via an operator who would manually record the details of each call. *Id.* at 1334–35.

As the automatic message accounting system was deployed throughout the United States beginning in the 1950s, it was necessary to centralize the accounting function due to the high cost of the infrastructure relative to the volume of toll calls at many

of the smaller local telephone offices. King, *supra*, at 1333; *see also* Phil Lapsley, *Exploding The Phone – Extras* (2013).[2] The automated message accounting system also evolved with the development of "automatic number identification" technology, which was deployed to ensure billing accuracy throughout the Bell System by 1961. *See* Robert J. Chapuis & Amos E. Joel, *100 Years of Telephone Switching, Part 2*, at 35 (2003). During the 1950s and 1960s, the Bell System continued to install and use centralized automatic message accounting systems, *see* Lapsley, *supra*, while Bell Laboratories conducted research into new electronic switching systems. Robert J. Chapuis & Amos E. Joel, *100 Years of Telephone Switching, Part 2*, at 48–56 (2003). The integration of digital computing technology into the telecommunications industry was ongoing throughout the 1970s, and the evolution of telecommunications services was rapid. *See id.* at 114–15. The first electronic switching system, No. 1 ESS, developed by Western Electric and Bell Laboratories, was put into operation in Succasunna, New Jersey in 1965. Each of the 24 Regional Bell Operating Companies had installed at least one ESS by 1967. *Id.* at 158. These electronic switching systems began using magnetic tape drives to store call detail information in the 1970s, but memory was limited and the storage of call details was necessarily temporary. *See id.* at 345.

In the 1970s there were no detailed records for most calls. Local call records were ephemeral because most customers paid a flat monthly rate and did not receive itemized bills. Robert G. Harris, *State Regula-*

---

[2] http://explodingthephone.com/extras/ama.php.

tory Policies and the Telecommunications/ Information Infrastructure in The Changing Nature of Telecommunications/Information Infrastructure (Computer Sci. & Telecomm. Bd. and Nat'l Research Council eds., 1995).

Even after the development of advanced electronic switching technologies, telephone companies had little incentive to store transactional data. By the mid-1970s, magnetic tape backup storage was integrated into the most advanced electronic switches. C.F. Ault, J.H. Brewster, T.S. Greenwood, R.E. Haglund, W.A. Read, & M.W. Rolund, *1A Processor: Memory Systems*, 56 Bell Sys. Tech. J. 181, 201 (1977). But there was little space to store phone records as bandwidth had to be preserved for other functions. That all changed after cell phone use became widespread and the government began requiring all wireless carriers to build increasingly accurate location tracking systems.

B. The pen register in *Smith* recorded only the outgoing numbers dialed by a single telephone customer.

Even the Court in *Smith* recognized that the pen registers had "limited capabilities." 442 U.S. at 741; *see also* Alan Butler, *Get A Warrant: The Supreme Court's New Course for Digital Privacy Rights After* Riley v. California, 10 Duke J. Const. L. & Pub. Pol'y 83, 101–05 (2014). The records in *Smith* did not reveal whether a call had been completed or whether any conversation took place. The Court in *Smith* relied on the definition of a pen register established in two earlier cases, which also emphasized the limited tracking ability of the device: *United States v. New York Telephone Company*, 434 U.S. 159 (1977), and

United States v. Giordano, 416 U.S. 505 (1974). *See Smith*, 442 U.S. at 736 n.1.

In these prior cases, the Court relied on the limited capability of a pen register in determining the application of the Wiretap Act. In *New York Telephone*, the Court rejected a phone company's challenge to an FBI pen register order. 434 U.S. at 165–66. The Court found that use of a pen register did not result in an "interception" of communications, and would "disclose only the telephone numbers that have been dialed." *Id.* at 167. In *New York Telephone*, the Court emphasized that "[n]either the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." *Id.*

Earlier, in *United States v. Giordano*, 416 U.S. 505 (1974), Justice Powell, writing for four members of the Court in dissent, also emphasized the limited capabilities of a pen register. The dissent argued that evidence collected by a pen register should not be suppressed because the device was "not governed by Title III." *Id.* at 553–54 (Powell, J., dissenting). Justice Powell stressed that the device "did not identify the telephone numbers from which incoming calls originated, nor does it reveal whether any call, either incoming or outgoing, was completed." *Id.* at 549 n.1.

Justice Powell's description of a pen register, which was relied upon by the Court in *Smith*, was based on the description of lower court in *Giordano*. *Id.* The lower court had found that a pen register was nothing more than a "decoder" used to translate electric tones generated during a phone's dialing operation. *United States v. Focarile*, 340 F. Supp. 1033, 1039 40 (D. Md. 1972). The rotary phone at issue in

Giordano signaled the numbers dialed when "a switch opened and closed a corresponding number of times to the digit dialed which in turn interrupt[ed] the direct current on the line and cause[d] the voltage of the electrical current to rise or fall the corresponding number of times." *Id.* at 1039. The pen register device, once installed on the phone line, would count "the number of pulses in the electrical energy caused by the changes in voltage, and cause[] the digit dialed on the telephone to be printed in Arabic numerals corresponding to the number of electric pulses." *Id.* A similar record could be generated for touch tone phone calls, though it required a more sophisticated technique. *Id.* at 1040.

Other courts reviewing pen register evidence during that period produced similar findings: pen registers only collected limited details about outgoing calls. *See, e.g., United States v. Caplan*, 255 F. Supp. 805, 807 (E.D. Mich. 1966) ("With reference to incoming calls, the pen register records only a dash for each ring of the telephone but does not identify the number from which the incoming call originated. The pen register cuts off after the number is dialed on outgoing calls and after the ringing is concluded on incoming calls without determining whether the call is completed or the receiver is answered.").

In 1979, when *Smith* was decided, a pen register log would show nothing more than the fact that a call was made at a specific time (e.g. 12:34 PM) to a specific number (e.g. 555-555-5555).

C. Location data for telephone users did not exist in the 1970s.

The contrast between the limited pen register records at issue in *Smith* and the cell phone location data in this case could not be more pronounced. A pen register in the 1970s could only record the number dialed by a target phone and the time the call was made. Most phones were not associated with an individual person, and a pen register could not even show whether any communication took place. Modern cell phone records include an entirely different category of information – location data—that can be used to map an individual's movements over time. That is precisely what happened in this case. The availability of increasingly precise location data underscores the need for a clear Fourth Amendment standard protecting against warrantless location tracking.

The privacy implications of cell phones arise from the structure of wireless communications networks. Unlike landline phones, cell phones generate precise location data that can be used to track an individual's movements over time. A cell phone is "a very sophisticated and versatile" device that uses radio waves to send and receive voice calls and data whenever it is within range of an antenna or tower. CTIA: The Wireless Association, *Wireless in America: How Wireless Works.*[3] Cell phones connect to a service provider's network via "cell sites," each of which contains a transceiver and controller used to relay signals between mobile devices and the network to enable calls and other communications. Axel Küpper,

---

[3] http://files.ctia.org/pdf/Brochure_HowWirelessWorks.pdf.

Location-Based Services: Fundamentals and Operation 91–97 (2006). *See generally* CDG, *Welcome to the World of CDMA: Glossary* (1999);[4] Tom Farley & Mark van der Hoek, *Cellular Telephone Basics* (2004).[5]

The data created when a cell phone communicates with a tower can be used to determine the location of the device and, in turn, the location of the person using the phone. Mobile devices communicate with nearby cell sites during a process called "registration," which occurs automatically even when the device is idle. *A Guide to the Wireless Engineering Body of Knowledge* 77 (Andrzej Jajszcyk ed., 2d ed. 2011). During the registration process, mobile devices ping nearby cell sites to identify the strongest signal. Michele Sequeira & Michael Westphal, *Cell Phone Science: What Happens When You Call and Why* 104 (2010).

A similar process occurs when a user moves from one cell site to another while making a call. Once registration occurs, the information is stored temporarily in service provider databases in order to route calls. Matt Blaze, *How Law Enforcement Tracks Cellular Phones* (Dec. 13, 2013).[6] Typically a log is created every time a call is made or data downloaded, *see* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location*

---

[4] http://www.cdg.org/technology/cdma_technology/a_ross/DefAtoF.asp.

[5] *Available at* https://web.archive.org/web/20041128222046/http://www.privateline.com:80/cellbasics/Cellbasics.pdf.

[6] http://www.crypto.com/blog/celltapping/.

Data that Congress Could Enact, 26 Berkeley Tech. L.J. 117, 128 (2012), including when smart phone apps access the internet without a user's knowledge. Sequeira & Westphal, *supra*.

Law enforcement investigators use this data to pinpoint the locations of people they are tracking. As Professor Laura Donohue has explained, "[s]ervice providers record where users' mobile devices connect to local towers— and not just when a telephone call is made or a text message is received, but constantly, as the user moves through space. The information provides a picture of where individuals go." Laura Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. Ann. Surv. Am. L. 553, 618–19 (2017). Maps can be created and introduced as evidence. In this case, the United States submitted maps and a report from the FBI's "Cellular Analysis Survey Team." *See* SA Christopher J. Hess, Detroit Division, Detroit Major Crimes Task Force, *Cellular Analysis* (Nov. 5, 2013), ECF No. 211-2.

Location data can precisely locate an individual because (1) cell phones "constantly scan their environment looking for the best signal," and (2) "the best signal generally comes from the tower that is CLOSEST to the phone, or is in direct LINE OF SIGHT." *Id.* at 5. The records show which cell site the target was connected to when each call was initiated and when each call ended. *Id.*

These cell site records reveal more than whether a user was somewhere near a tower. Cell towers typically have three 120° "sectors," and the antennas "have a downwards tilt" such that each sector covers the area of "an upside-down funnel." *Id.* 5–6. By comparing the cell site records with tower loca-

tion and sector data, law enforcement can generate precise location data that can be visualized using computer mapping software. *See, e.g., id.* at 11–15.[7]

Cell site location information is not the only type of location data that has been seized in criminal cases. In addition to historical cell site location information, officers often seize cell site and GPS data in real time. *See, e.g., United States v. Wallace*, ___ F.3d ___, 2017 WL 3304087 (5th Cir. 2017) (officer used a "Ping Order" to "obtain real-time geolocation coordinates"); *United States v. Barajas*, 710 F.3d 1102 (10th Cir. 2013) (DEA agent obtained from the cell phone provider "GPS coordinates for the location of [the] telephone within a certain radius" in real time).

Cell phone providers have developed real-time location tracking methods to comply with regulations

---

[7] Hannah Arendt warned that such capability would enable the emergence of a totalitarian state:

> Now the police dreams that one look at the gigantic map on the office wall should suffice at any given moment to establish who is related to whom and in what degree of intimacy; and, theoretically, this dream is not unrealizable although its technical execution is bound to be somewhat difficult. If this map really did exist, not even memory would stand in the way of the totalitarian claim to domination; such a map might make it possible to obliterate people without any traces, as if they had never existed at all.

Hannah Arendt, *The Origins of Totalitarianism* 434 (1973).

that require providers to be able to locate a 911 caller in an emergency. *See* 47 C.F.R. § 20.18. The FCC has increased the location accuracy requirements in the decades since they were first introduced as users have transitioned from land lines to mobile phones. Wireless E911 Location Accuracy Requirements, *Third Further Notice of Proposed Rulemaking*, 29 FCC Rcd 2374 ¶1 (2014) ("[T]oday, the majority of 911 calls come from wireless phones."). The FCC now requires that providers be able to accurately locate users indoors. Wireless E911 Location Accuracy Requirements, *Fourth Report and Order*, 30 FCC Rcd 1259 ¶ 1, 6 (2015). All providers must have the capability to pinpoint a 911 caller within 50 meters horizontally and develop a method for establishing vertical ("z-axis") location data as well. *Id.* ¶ 6.

Providers currently use triangulation (or "lateration") methods based on the simultaneous signals received by different base stations. *See* Ali H. Sayed, Alireza Tarighat & Nima Khajehnouri, *Network-Based Wireless Location*, IEEE Signal Processing Magazine 24, 26–29 (Jul. 2005); *see also* Axel Küpper, *Location-Based Services: Fundamentals and Operation* 131–36 (2006). An even more precise location record can be calculated using the exact angle and time of arrival of each signal. *See id.* at 138–40, 144–48. One example of such a system is the U-TDOA technique implemented by Skyhook and used by current mobile carriers. Dave McHoul, *Locating a 911 Caller*, Skyhook (June 2, 2016).[8] In response to the FCC's "indoor mandate," providers are deploying new

[8] http://blog.skyhookwireless.com/precision/location/locating-a-911-caller.

techniques that can locate a device even when the call is placed indoors. *Id.* "[T]he line between public and private modes of surveillance and security has blurred if not vanished." Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1, 7 (2008).

The use and disclosure of emergency call data is restricted under the Federal Communications Act, which mandates that service providers protect consumer privacy by limiting disclosure of consumer proprietary network information ("CPNI"). *See* 47 U.S.C. § 222.[9] Despite the fact that the E-911 system was developed to be used for emergencies, law enforcement has demanded access to the same data for criminal enforcement purposes. *See, e.g.*, *Barajas*, 710 F.3d at 1104 n.1.

Although the Court observed in *Smith* that "[n]umbers dialed to and from a phone are not entitled to as much privacy protection as the content of the conversation," *Smith*, 442 U.S. at 735, "[i]n 2014 the opposite is true. Most cell conversations are not probative, not sensitive, not revealing. But the numbers dialed to us and from us show our associations and our patterns." Robert Ellis Smith, *Location Location Location* 3 (2014). Indeed, as computer security expert Bruce Schneier has explained, "location data is so valuable that cell phone companies are now selling it to data brokers, who in turn resell it to anyone

---

[9] There are only three exceptions to the CPNI rule that allow disclosure of cell phone location information: (1) to an emergency 911 service, (2) to inform a legal guardian in an emergency, and (3) to assist in the delivery of emergency services. 47 U.S.C. § 222(d)(4).

willing to pay for it." Bruce Schneier, *Data and Goliath* 2 (2015).[10] National Constitution Center President Jeffrey Rosen, writing about similar issues before the Court in *Jones*, and acknowledging the views of Judge Douglas Ginsberg, warned that "[i]f the court rejects his logic and sides with those who maintain that we have no expectation of privacy in our public movements, surveillance is likely to expand, radically transforming our experience of both public and virtual spaces." Jeffrey Rosen, *Protect Our Right to Anonymity*, N.Y. Times, Sept. 13, 2011, at A31.

Justice O'Connor has also emphasized the need to maintain constitutional safeguards as new technologies emerge. "With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities." *Arizona v. Evans*, 514 U.S. 1, 17–18 (1995) (O'Connor, J., concurring). And as Justice Scalia explained for the Court in *Kyllo v. United States*:

> It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. . . . The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.

533 U.S. 27, 33–34 (2001).

Justice Scalia concluded in *Kyllo* that the use of a thermal imaging device to record activities inside the home would "permit police technology to erode the privacy guaranteed by the Fourth Amendment,"

---

[10] http://www.educause.edu/ir/library/pdf/LIVE1402.pdf.

and must therefore be considered a search. *Id.* at 34. "This assures," as Justice Scalia explained, "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.*; *see also United States v. Denson*, 775 F.3d 1214 (10th Cir. 2014) ("New technologies bring with them not only new opportunities for law enforcement to catch criminals but also new risks for abuse and new ways to invade constitutional rights.").

D. The Court recognized in *Riley* that modern communications services store a wealth of sensitive personal data.

Location information is just one element in the constellation of sensitive data that cell phone users regularly entrust to service providers. As the Court explained in *Riley*, modern cell phones are used to create, receive, and access a "broad array of private information," *Riley*, 134 S. Ct. at 2491:

> The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers. . . . . Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on. . . . Data on a cell phone can also reveal where a person has been. Historic location information is

> a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.

Id. at 134 S. Ct. at 2489–90. Moreover, much of the private data created and accessed with cell phones is actually stored on remote servers:

> To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. . . . Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.

Id. (citing Brief for Electronic Privacy Information Center at 12–14, 20, *Riley*, 134 S. Ct. 2473 (No. 13–132)). "So much digital information, misinformation, data, and garbage is being squirreled away . . . . And computers are getting better and better at extracting meaning . . . sometimes reveal[ing] things about us we did not expect others to know." Hal Abelson, Hen Ledeen, & Harry Lewis, *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion* 2 (2008). "[W]e are rapidly adopting personal service robots . . . . They see what we point them at; they have ears to hear everything going on around us; they know our location all the time. These robots we call smartphones and tablets often contain software we cannot read or understand, much less change."

Eben Moglen, *The Tangled Web We Have Woven*, 56 Comms. ACM 20, 21 (2013).

Given the sensitive nature of the cell phone data that is stored remotely and this Court's requirement that the Government obtain a warrant before conducting a search of a phone, *Riley*, 134 S. Ct. at 2495, it would be illogical to hold that the same data, once uploaded to a remote server, is no longer protected. Yet that is the sweeping implication of the Government's argument that it can collect cell phone location data without a warrant. Sensitive personal data—photos, emails, location information, or otherwise—does not become less private simply because a cell phone user entrusts that information to a communications service provider.

II. Cell phone users do not "assume the risk" that their personal data will be disclosed to others.

Extending the concept of "assumption of risk," relied upon by the Court in *Smith*, to cell site location information would ignore technological changes and defy common sense.

In *Miller*, the Supreme Court concluded that an individual "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *United States v. Miller*, 425 U.S. 435, 443 (1976). In *Smith*, the Court extended this logic to call detail records based on a finding that the defendant "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business . . . assum[ing] the risk that

the company would reveal to police the numbers he dialed." *Smith*, 442 U.S. at 744.

Yet this "assumption of risk" construct does not apply to the modern cell phone user. Consumers do not assume the risk that their personal data will be disclosed by their cell phone providers simply because of their participation in an essential part of modern life. In the reality, cell phone users now make exactly the opposite assumption. Survey data demonstrates that individuals expect their personal data to be kept private by their service providers.

A. Cell phone users expect that their personal data will be kept private.

Particularly important for the case before this Court, mobile phone users today are concerned about the collection and use of their location data. In *Smith*, Justice Marshall wrote in dissent that "unless a person is prepared to forgo" the telephone, for "many . . . a personal or professional necessity, he cannot help but accept the risk of surveillance." *Smith*, 442 U.S. at 750 (Marshall, J., dissenting). He concluded that "[i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." *Id.*

This warning has proved prescient. Cell phones are an essential part of modern life. Americans use them for purposes ranging from the intimate to the mundane; the devices are often in our pockets, purses, or backpacks everywhere we travel—from church, to school, to home, to the political rally, and the doctor's office. In opinion surveys, Americans express deep concerns about data privacy, skepticism

about companies' business practices, and a desire for limits on location data tracking.

Americans rely on cell phones to participate in life. 95% of Americans own a cell phone. *Mobile Fact Sheet*, PewResearch Center (Jan. 12, 2017).[11] That number rises to 100% for 18- to 29-year-olds. *Id.* 84% of American households have at least one smart phone, and a third have three or more. Kenneth Olmstead, *A Third of Americans Live in a Household with Three or More Smartphones*, PewResearch Center (May 25, 2017).[12] Phones are also the sole source of internet access at home for one in ten Americans, a trend that is even stronger among younger, non-white, and lower-income Americans. *Mobile Fact Sheet*, PewResearch Center (Jan. 12, 2017).[13] A recent study shows that now "a majority of American homes ha[ve] only wireless telephones." Stephen J. Blumberg & Julian V. Luke, Nat. Cent. for Health Statistics, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July–December 2016* at 1 (2017).

A 2016 PewResearch survey documents that Americans are deeply concerned about privacy. Pew discovered that "65% of Americans say there are not adequate limits on 'what telephone and internet data the government can collect.'" Lee Rainie, *The State of Privacy in Post-Snowden America*, PewResearch Cen-

---

[11] http://www.pewinternet.org/fact-sheet/mobile/.

[12] http://www.pewresearch.org/fact-tank/2017/05/25/a-third-of-americans-live-in-a-household-with-three-or-more-smartphones/.

[13] http://www.pewinternet.org/fact-sheet/mobile/.

ter (Sept. 21, 2016).[14] Pew also found that individuals are trying to protect their privacy: "86% of Internet users have taken steps online to remove or mask their digital footprints." *Id.* A majority of users (61%) say they would like to do more to protect their personal information online. *Id.* Users certainly do not consent to location tracking; only 52% of those surveyed understood "that turning off the GPS function of a smartphone *does not* prevent all tracking of that device." Kenneth Olmstead & Aaron Smith, *What the Public Knows About Cybersecurity*, PewResearch Center (Mar. 22, 2017).[15]

According to the Pew survey, a clear majority of Americans say that it is "very important" to be "in control of who can get information about them" and "to control what information is collected about them." Rainie, *supra*. Yet Americans also "express a consistent lack of confidence" that that "records will remain private and secure," and 56% are either not too confident or not at all confident that cell phone companies adequately protect their records. *Id.*

Young adults between 18 and 29 "generally are more focused than their elders when it comes to online privacy." *Id.* And while "younger adults are more likely to have shared personal information," that does not negate their privacy concerns. *Id.* In fact, the opposite is true. This group is most likely to "have paid attention to privacy issues." *Id.* Similarly, they are more likely to have taken active steps to pro-

---

[14] http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

[15] http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/.

tect their privacy such as "limit[ing] the amount of personal information available about them online, chang[ing] privacy settings, delet[ing] unwanted comments on social media, remov[ing] their name from photos in which they were tagged, and tak[ing] steps to mask their identities while online." *Id.*

Many users say that their privacy is at risk when location or travel data is gathered by a third party. Those numbers increase to substantial majorities when that data is later shared with law enforcement agencies without a warrant. In one survey, for instance, 51% of respondents indicated they either agreed or strongly agreed that having "location or travel data collected and stored by a private company (such as Google)" placed their privacy at risk. Caitlin D. Cottrill & Piyushimita "Vonu" Thakuriah, *Location Privacy Preferences: A Survey-based Analysis of Consumer Awareness, Trade-off and Decision-making*, 56 Transp. Res. Part C 132 (2015). Over 71% of respondents either agreed or strongly agreed that their privacy would be placed at risk by "[h]aving location or travel information gathered by a private company . . . shared with law enforcement agencies with no warrant issued" as the government seeks to do here. *Id.*

In short, the privacy interests of Americans have not diminished with the widespread use of cell phones. Instead, consumers express concern and seek to protect their personal data. Far from "assuming the risk" associated the new technology, cell phone users reasonably expect that the records of their activities will be protected.

B. Cell phone users limit access to their location data.

At the time *Smith* was decided, there was no extrinsic evidence about individual users' expectations regarding the privacy of the numbers dialed; users had no choice if they wanted to make a call. But in the era of smart phones, users have a wide range of tools and settings available to enhance the privacy of their cell phone data. Responding to demand, mobile companies and apps are increasing the availability of location privacy controls. Today, these controls are basic privacy features of all major cell phone models and mobile applications. The availability of location settings demonstrates that individuals are not, in any meaningful way, "assuming the risk" that their location data will be revealed by service providers. Instead, users are taking active steps to maintain privacy of their personal data.

The Apple iPhone allows users to disable location services for the device entirely. Apple, *About Location Services and Privacy*, Apple Support (June 21, 2017).[16] These safeguards in the modern cell phone follow almost directly from concerns expressed by users about location tracking.

In 2011 Apple faced pressure after two security researchers revealed Apple was routinely storing location data in hidden files on iPhones and iPads. The pair found that Apple devices running iOS 4 consistently recorded time-stamped latitude-longitude coordinates. Alisdair Allan & Peter Warden, *Got an iPh-*

---

[16] https://support.apple.com/en-us/HT207056.

one or 3G iPad? Apple is Recording Your Moves, O'Reilly Radar (Apr. 20, 2011).[17] Moreover, the data was stored in an unencrypted file called "consolidated.db," which could easily be compromised by third parties. *Id.* The data logs tracked as much as a year's worth of movements—the time between release of the operating system and the security flaw's discovery—and the data cache was transferred for backup purposes anytime the device was synced. *Id.*

EPIC had previously warned about the expansion of location tracking by Apple and other companies. *See* Statement for the Record from EPIC, Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services before the Subcomm. on the Constitution, Civil Rights, & Civil Liberties, of the House Comm. on Judiciary (June 24, 2010).[18]

Users were outraged when they learned about this surreptitious location tracking. *See* EPIC, *iPhones, iPads Collect and Store User Location Data* (Apr. 21, 2011).[19] Representative Edward Markey wrote to Steve Jobs the next day, demanding answers to questions about the data collection. "Apple needs to safeguard the personal location information of its users to ensure that an iPhone doesn't become an iTrack." Press Release, Markey to Apple: Is It iPhone

---

[17] http://radar.oreilly.com/2011/04/apple-location-tracking.html.

[18] https://epic.org/privacy/ECPA_Statement_2010-06-24.pdf.

[19] https://epic.org/2011/04/post-10.html.

or iTrack? (April 21, 2011).[20] The Congressman pressed the company about compliance with user consent requirements of § 222 of the Communications Act. *Id.* Senator Al Franken also wrote to the CEO asking for a "prompt response" to a series of questions, including why this data was compiled in the first place and why the company failed to secure it. Letter from Sen. Al Franken to Steve Jobs, CEO of Apple (Apr. 20, 2011).[21] A class action lawsuit was filed against the company in district court alleging violations of the Computer Fraud and Abuse Act and state unfair and deceptive trade practice laws. *See In re iPhone Application Litigation*, 6 F. Supp. 3d 1004 (N.D. Cal. 2013).

In response to the public outcry, "Steven P. Jobs, Apple's chief executive, took the unusual step of personally explaining that while Apple had made mistakes in how it handled location data on its mobile devices, it had not used the iPhone and iPad to keep tabs on the whereabouts of its customers." Miguel Helft, *Jobs Said Apple Made Mistake with iPhone Data*, N.Y. Times, Apr. 27, 2011, at B3. According to the New York Times, Jobs stated, "We haven't been tracking anybody. Never have. Never will." *Id.*

Within a week, the company announced it would release a software update to address privacy and data security concerns. Press Release, Apple

---

[20] https://www.markey.senate.gov/news/press-releases/april-21-2011-markey-to-apple-is-it-iphone-or-itrack.

[21] https://www.franken.senate.gov/files/letter/110420_Apple_Letter.pdf.

Q&A on Location Data (Apr. 27, 2011).[22] The update restricted storage of location data, stop the automated transfer of location data, and completely purged all location data when a user turned off location services. *Id.* The company also announced that the next major software release would encrypt cached location data. *Id.*

As the New York Times recounted the battle: "Some privacy advocates who were harshly critical of Apple last week praised the company's response, saying it was a step in the right direction." Helft, *supra*. The Times also quoted EPIC Executive Director Marc Rotenberg as stating, "Apple acknowledged a mistake and they fixed it. . . . That's a good thing." *Id.*; *see also Washington Journal: Cell Phone Tracking and Privacy Issues* (C-SPAN Apr. 26, 2011).[23]

In sum, cell phone users today have made clear their strong belief in privacy protections, so much so that the CEO of the company that produces the most popular cell phone in the world was required to respond quickly when the company inadvertently collected location data.

---

[22] https://www.apple.com/newsroom/2011/04/27Apple-Q-A-on-Location-Data/.

[23] https://www.c-span.org/video/?299201-4/cell-phone-tracking-privacy-issues.

III. This Court must determine the appropriate scope of the Fourth Amendment. Then it is for Congress to develop an appropriate statutory framework.

The Court and Congress have long worked together to determine the scope of the right to privacy. Marc Rotenberg & David Brody, *Protecting Privacy: The Role of the Courts and Congress*, Hum. Rts., March 2013, at 7, 10. ("Both courts and Congress share responsibility for safeguarding individuals' privacy from advancing technology and overzealous government surveillance."). Congress brings the ability for detailed fact-finding and the development of clear rules set out in public law. "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." *Jones*, 565 U.S. at 427–28 (Alito, J., concurring) (internal citations omitted); *see also* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 Minn. L. Rev. 62, 110 (2013) ("[T]he law enforcement and privacy interests at stake can be explored in a more expansive and timely manner in the context of legislative or executive rule making processes than they can be in the context of constitutional litigation."); Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 Mich. L. Rev. 485, 535 (2013) ("Congress has proven more adept than the courts at implementing mechanisms for systemic oversight of privacy

practices, as well as for reform of noncompliant institutions.").

But Congress should follow the lead of the Court as new conflicts between law enforcement practices, emerging technology, and Fourth Amendment privacy protections emerge. Rotenberg & Brody, *supra*, at 10 ("Privacy protection under the Fourth Amendment is first and foremost the responsibility of the courts."). With the Court's constitutional guidance, Congress can take its turn and enact privacy legislation "that draws reasonable distinctions based on categories of information or [] other variables." *Riley*, 134 S. Ct. at 2497.

"The regulation of electronic surveillance provides an instructive example" of Congress's complementary role in defining privacy protections. *Id.* In 1967, the Court struck down a New York statute because it permitted electronic eavesdropping "without requiring belief that any particular offense ha[d] been or [was] being committed" and without requiring that the "conversations [sought] be particularly described." *Berger v. New York*, 388 U.S. 41, 58–59 (1967). Later that term, the Court held that warrantless eavesdropping on a telephone booth violated the Fourth Amendment because it intruded on the caller's reasonable expectation of privacy. *Katz v. United States*, 389 U.S. 347, 358–59 (1967); *id.* at 360 (Harlan, J., concurring).

It was only after the landmark *Berger* and *Katz* decisions that Congress developed a comprehensive statutory framework governing electronic surveillance. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, Tit. III, 82 Stat. 197,

211–25 (codified as amended at 18 U.S.C. §§ 2510–20). In drafting Title III, Congress expressly relied on the factors that the Court had set out in *Berger* and *Katz*. S. Rep. No. 90-1097, 73–75 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2161–63 ("Working from the hypothesis that any wiretapping and electronic surveillance legislation should include . . . constitutional standards, the subcommittee has used the *Berger* and *Katz* decisions as a guide in drafting title III."). "It was the Court's decision in 1967 that set the course for the modern right to privacy, but it was the congressional legislation the following year that gave meaning to that right." Rotenberg & Brody, *supra*, at 10.

This dialogue between the Court and Congress continued into the 1970s over the issue of national security surveillance. In *United States v. U.S. Dist. Court for Eastern Dist. of Mich.*, 407 U.S. 297 (1972) (*Keith*), the Court held that the Fourth Amendment requires the government to comply with an "appropriate prior warrant procedure" before conducting surveillance for domestic security purposes. *Id.* at 320. The distinction drawn by the *Keith* Court between surveillance of foreign and domestic parties was foundational to Congress's enactment of the Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801 *et seq.*). As the Senate Report explained, the statute would "not authorize electronic surveillance under any circumstances for the class of individuals included by the Supreme Court within the scope of the *Keith* decision requiring judicial warrants for alleged threats to security of a domestic nature." S. Rep. No. 95-604, pt. 1, at 26 (1978), *as re-*

printed in 1978 U.S.C.C.A.N. 3904, 3928. Congress thus took its constitutional cues from the Court's Fourth Amendment jurisprudence.

Justice Alito, as a college student, even anticipated this development. Writing in 1972 as the *Keith* case was ongoing, Justice Alito set out the contours of federal legislation for a court of national security warrants:

> A Federal Court of Warrants should be created to issue warrants for electronic surveillance in *all* cases involving the national security. . . . Recognizing both that the usual procedures may be inappropriate in cases involving the national security and that the system proposed by the government is highly susceptible to abuses, we propose that a Federal Court of Warrants be created solely for the purpose of hearing these cases.

Samuel Alito et al., Final Report, *in Conference on the Boundaries of Privacy in American Society* 6, 10–11 (1972).[24] Within seven years, Congress had enacted the FISA and established the Foreign Intelligence Surveillance Court. 50 U.S.C. § 1803.

The Court remains the interpreter of the Fourth Amendment in our modern age. The government's practice of obtaining cell phone location data without a warrant is out of step with the Court's recent opinions. The Court can and should leave the work of "impos[ing] detailed restrictions on electronic surveillance" to Congress, as it has done before. *Ri-*

---

[24] https://www.epic.org/privacy/justices/alito/princeton/.

ley, 134 S. Ct. at 2497. But the Court should first establish that the Fourth Amendment applies to cell phone location data. It is "emphatically the province and duty of the judicial department to say what the law is." *Marbury v. Madison*, 5 U.S. 137, 177 (1803).

CONCLUSION

For the foregoing reasons, *amici* respectfully ask this Court to reverse the decision of the U.S. Court of Appeals for the Sixth Circuit.

Respectfully submitted,

MARC ROTENBERG
ALAN BUTLER
JOHN DAVISSON
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
(202) 483-1248 (fax)
rotenberg@epic.org

August 14, 2017

RECORD AND BRIEFS

FILED
AUG 14 2017
OFFICE OF THE CLERK
SUPREME COURT, U.S.

No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES,

Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Sixth Circuit

BRIEF OF *AMICI CURIAE* EMPIRICAL FOURTH AMENDMENT SCHOLARS IN SUPPORT OF PETITIONER

SARAH O'ROURKE SCHRUP *
JEFFREY T. GREEN
NORTHWESTERN SUPREME COURT PRACTICUM
375 East Chicago Avenue
Chicago, IL 60611
(312) 503-0063
s-schrup@law.northwestern.edu

Counsel for Amici Curiae

* Counsel of Record

August 14, 2017

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES	ii
INTEREST OF *AMICI CURIAE*	1
SUMMARY OF THE ARGUMENT	1
ARGUMENT	2
I. EMPIRICAL RESEARCH DEMONSTRATES THAT PEOPLE MAINTAIN AN EXPECTATION OF PRIVACY IN THEIR HISTORICAL CELL SITE LOCATION INFORMATION	2
A. The Presumption Employed By The Court Below And Other Courts Of Appeals In Order To Invoke The Third Party Doctrine Is Belied By Statistical Evidence	2
B. Research Demonstrates That Most People Have An Expectation Of Privacy In Both Cell Site Location Information And GPS Location Information	4
II. THE DATA ARE DOCTRINALLY SIGNIFICANT IN THIS COURT'S FOURTH AMENDMENT JURISPRUDENCE	10
CONCLUSION	16

TABLE OF AUTHORITIES

CASES

Page

In re Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) 3
Ballew v. *Georgia*, 435 U.S. 223 (1978) 12
Brandin v. *State*, 669 So. 2d 280 (Fla. Dist. Ct. App. 1996) 12
Brown v. *Bd. of Educ. of Topeka*, 347 U.S. 483 (1954) 12
California v. *Ciraolo*, 476 U.S. 207 (1986) 10
City of Ontario v. *Quon*, 560 U.S. 746 (2010) 10
Commonwealth v. *Johnson*, 75 N.E.3d 51 (Mass. App. Ct. 2017) (Wolohojian, J., dissenting) 12
Florida v. *Jardines*, 133 S. Ct. 1409 (2013) 10, 11
In re Gault, 387 U.S. 1 (1967) 12
Georgia v. *Randolph*, 547 U.S. 103 (2006) 10
Katz v. *United States*, 389 U.S. 347 (1967) (Harlan, J., concurring) 4
Kyllo v. *United States*, 533 U.S. 27 (2001) 11, 14
Love v. *State*, NO. AP-77,024, 2016 WL 7131259 (Tex Ct. Crim. App. Dec. 7, 2016), *reh'g denied* (Apr. 12, 2017) 12, 13
Minnesota v. *Olson*, 495 U.S. 91 (1990) 10
Rakas v. *Illinois*, 439 U.S. 128 (1978) 11
Smith v. *Maryland*, 442 U.S. 735 (1979) 10, 15
United States v. *Carpenter*, 819 F.3d 880 (6th Cir. 2016) 2, 4
United States v. *Davis*, 785 F.3d 498 (11th Cir. 2015) (en banc) 2, 3

TABLE OF AUTHORITIES—continued

Page

United States v. *Jacobsen*, 466 U.S. 109 (1984) 11

United States v. *Jones*, 565 U.S. 400 (2012) 11

United States v. *Leon*, 468 U.S. 897 (1984) 12

COURT DOCUMENT

Transcript of Oral Argument, *Brendlin* v. *California*, 551 U.S. 249 (2007) (No. 06-8120) 12

OTHER AUTHORITIES

Alisa Smith, Sean Madden & Robert P. Barton, *An Empirical Examination of Societal Expectations of Privacy in the Digital Age of GPS, Cell Phone Towers, & Drones*, 26 Alb. L.J. Sci. & Tech. 111 (2016) 8, 9

Bernard Chao, Catherine S. Durso, Ian P. Farrell & Christopher T. Robertson, *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 Cal. L. Rev. (forthcoming 2018) 7, 14

Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 Wake Forest L. Rev. 261 (2014) 4, 5

Christine S. Scott-Hayward, Henry F. Fradella & Ryan G. Fischer, *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 Am. J. Crim. L. 19 (2015–2016) 8, 9, 16

TABLE OF AUTHORITIES—continued

Page

Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (2007) 14, 16

Christopher Slobogin, *Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire*, 94 Minn. L. Rev. 1588 (2009–2010) 13

Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 Duke L.J. 727 (1993) 15

Erwin Chemerinsky, *Rediscovering Brandeis's Right to Privacy*, 45 Brandeis L.J. 643 (2006–2007) 14

Janice Nadler, *No Need to Shout: Bus Sweeps and the Psychology of Coercion*, 2002 Sup. Ct. Rev. 153 (2002) 13

Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 Sup. Ct. Rev. 205 (2015) ..... *passim*

Matthew B. Kugler & Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U. Chi. L. Rev. (forthcoming 2017) 15

Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 Nw. U. L. Rev. 139 (2016) 3, 4

TABLE OF AUTHORITIES—continued

Page

Orin S. Kerr, *Do We Need a New Fourth Amendment?*, 107 Mich. L. Rev. 951 (2009) 13

Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era* (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf 5

Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 Sup. Ct. Rev. 173 (1979) 14

Shari Seidman Diamond & David J. Franklyn, *Trademark Surveys: An Undulating Path*, 92 Tex. L. Rev. 2029 (2014) 12

Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. Legal Stud. 1 (2014) 4

INTEREST OF *AMICI CURIAE*[1]

Amici are professors (identified in the Appendix) whose research and teaching include the Fourth Amendment, empirical analysis of the criminal justice system, and, specifically, empirical analyses of the public's "reasonable expectations." They file this brief to urge this Court to reverse the Sixth Circuit, recognize that the Fourth Amendment governs the inquiry here, and find that authorities violate the Fourth Amendment when law enforcement collect cell site location data without first obtaining a warrant.

SUMMARY OF THE ARGUMENT

The Court has recognized that public expectations of privacy are relevant to the Fourth Amendment. A growing body of social science research shows that a majority of people: (1) do not knowingly convey their location information to cell phone providers; and (2) believe that law enforcement needs to obtain, and ought to obtain, a search warrant before gathering this information. These studies addressed a range of surveilled information (cell site location and GPS tracking) and conduct (by cell phone providers and by law enforcement). On average across all the studies more than 60% of survey respondents (and often upwards of 70-80%) emphatically asserted a privacy interest in the information contained on or emitted from their cell phones. In relative terms, these priva-

---

[1] In accordance with Supreme Court Rule 37.3, *amici curiae* states that no counsel for any party to these proceedings authored this brief, in whole or in part. No entity or person, aside from *amici curiae*, its members, and its counsel, made any monetary contribution for the preparation or submission of this brief. Petitioner and Respondent have consented to the filing of this brief. Letters reflecting such consent have been filed with the Clerk.

cy interests are as strong, or stronger, than paradigmatic cases where the Court has required law enforcement officials to first obtain a warrant.

These empirical data, detailed below, expressly undercut the Sixth Circuit's reliance on the third party doctrine in deciding this case, and affirmatively support a finding that warrantless searches of this information violate the Fourth Amendment. This Court should employ these empirical data—a critical tool that informs the proper scope and functioning of the Fourth Amendment—and reverse the decision below.

ARGUMENT

I. EMPIRICAL RESEARCH DEMONSTRATES THAT PEOPLE MAINTAIN AN EXPECTATION OF PRIVACY IN THEIR HISTORICAL CELL SITE LOCATION INFORMATION.

A. The Presumption Employed By The Court Below And Other Courts Of Appeals In Order To Invoke The Third Party Doctrine Is Belied By Statistical Evidence.

In relying on the third party doctrine to dispose of Mr. Carpenter's case, the Sixth Circuit presumed that citizens knowingly and voluntarily reveal their cell site location information to third party cell phone providers. *United States* v. *Carpenter*, 819 F.3d 880, 888–89 (6th Cir. 2016) (citing *United States* v. *Miller*, 425 U.S. 435, 442 (1976) and *Smith* v. *Maryland*, 442 U.S. 735 (1979)). Other courts of appeals have similarly found that cell site location information falls outside the bounds of Fourth Amendment protection under the third party doctrine. See, *e.g.*, *United States* v. *Davis*, 785 F.3d 498, 511 (11th Cir. 2015) (en banc) (cell phone users "know . . . that cell phone

companies make records of [their] cell-tower usage"); *In re Historical Cell Site Data*, 724 F.3d 600, 612 (5th Cir. 2013) ("[U]sers know that they convey information about their location to their service providers when they make a call and . . . they voluntarily continue to make such calls.").

This presumption, however, is undermined by empirical research. In one recent study, only 26.5% of American cell phone users expressed even a general awareness that their cell phone companies may track their locations. Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 Nw. U. L. Rev. 139, 177 (2016). Specifically, when 841 adult cell phone users were asked whether their "cell phone service provider regularly collect[ed] information on your physical location using your cell phone", 73.5% of respondents answered either "No" (15.0%) or "I Don't Know" (58.5%).[2] *Id.* The 26.5% of participants who answered "Yes" were then asked an open-ended follow-up question: "Please describe how your cell phone service collects information on your physical location." Even with the most liberal coding—any response that could reasonably be interpreted as referring to cell site location tracking was counted as doing so—only 12.7% of this "Yes"-answering subset

---

[2] Participants were recruited through M-Turk, an online workforce commonly used for survey and experimental research. The sample was not nationally representative and compared with 2010 census data, was more male (53.5% compared with 49.2%), younger (for example, 56.2% of participants were between ages 18–34 compared with 30.6% of the U.S. population), and better educated (for example, 46.7% of participants had a bachelor's degree or higher compared with 27.3% of the U.S. population).

could be deemed to have been referring to cell-site tracking. *Id.*[3]

Thus, although lower courts have been quick to attribute to cell phone users both knowledge and the voluntary display of cell site information, the data shows otherwise. Compare *Carpenter*, 819 F.3d at 888 ("any cellphone user who has seen her phone's signal strength fluctuate must know that, when she places or receives a call, her phone 'exposes' its location to the nearest cell tower and thus to the company that operates the tower"), with Tokson, *supra* p. 3, at 164–66, 179 ("results . . . suggest[ing] that many courts have imputed knowledge about cell phone technology and surveillance practices that users do not possess").

B. Research Demonstrates That Most People Have An Expectation Of Privacy In Both Cell Site Location Information And GPS Location Information.

Empirical research likewise informs the threshold Fourth Amendment inquiry of whether a reasonable expectation of privacy exists in cell site location data. *Katz* v. *United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). A substantial set of empirical research demonstrates that people generally expect privacy in this domain. Some studies focus on the general question of privacy interests in electronic de-

---

[3] Nor could knowledge and voluntariness be gleaned from cell service providers' official privacy policies because 89.8% of respondents neither read the policy nor even skimmed it in detail. *Id.* at 178; *accord* Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. Legal Stud. 1, 20 (2014) (in the user-clickstream data context, confirming that actual reading of user agreements and privacy policies is even lower than rates of self-reporting).

vices more broadly. See, *e.g.*, Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 Wake Forest L. Rev. 261 (2014); see also Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era* 34–35 (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf (finding that people often think of privacy interests in their devices as extremely sensitive, on a level with their privacy interests in their homes). Other studies—including the four discussed below—have expressly dealt with privacy interests in cell site location and, relatedly, GPS tracking data. Although these projects approached the question of privacy expectations somewhat differently and surveyed a slightly different mix of the national population, the result was always the same: more people expect privacy in their cell-site location information than do not.[4]

Several studies focused in whole or in part on the mere collection of cell phone data, in both the cell site location and GPS contexts. The studies also variously considered historic and real-time surveillance. In one study, scholars asked a nationally representative sample[5] of 739 U.S. citizens whether it would "violate people's reasonable expectations of privacy if law en-

---

[4] The expectation of privacy was generally stronger in the GPS tracking context than in the cell site location context because these surveys often implied that GPS tracking was more precise (and thus more invasive), but the expectation was strong in both domains and in all the studies.

[5] In other words, their sample mirrored the U.S. adult citizen population in terms of gender, race, and age. Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 Sup. Ct. Rev. 205, 245 n.162, 256 n.188 (2015) ("*Actual Expectations of Privacy*").

forcement . . . obtained from their cell-phone company stored information about whether their cell phone was near a particular location on a particular day." *Actual Expectations of Privacy, supra* note 5, at 258–60. Forty-nine percent reported that this conduct violated their expectations of privacy, while 31% said it did not, and 20% remained neutral. *Id.* at 260. That study also examined real-time GPS tracking and showed that a majority believes this practice also infringes on their privacy rights, and does so even in cases of very short-term tracking. Respondents were asked whether it would violate people's reasonable expectations of privacy if police "used a car's onboard GPS system" to (1) locate it, and (2) track it (for one day, one week, and one month). Depending on the duration of the surveillance, between 54% and 63% of participants reported that it would, as opposed to the range of respondents (19%-27%) who said it would not. *Id.* at 257. Notably, a follow-up study randomly varied the phrasing of the questions, asking respondents about "expectations of privacy," "reasonable expectations of privacy," or merely "privacy." Researchers found that altering the phrasing of the questions had no significant effect on the results. *Id.* at 248. No matter how the questions were phrased, a substantial majority of Americans believed GPS surveillance of any duration conflicted with their expectations of privacy and outnumbered by a 25-30% margin those who did not view it as intrusive. *Id.* at 257–58.[6]

A separate 1,200-person study that phrased the questions differently found that 85% of people believed it would violate their expectations of privacy if

---

[6] The same follow-up showed that changing the wording from the third person ("people's" expectations) of privacy to the first person ("your" expectation of privacy) increased privacy expectations somewhat. *Id.* at 248–49.

the police obtained from their cellphone provider their location data for a 7-month period.[7] Bernard Chao, Catherine S. Durso, Ian P. Farrell & Christopher T. Robertson, *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 Cal. L. Rev. (forthcoming 2018).[8] That same study gave participants a scenario in which police attached a GPS tracker to the bottom of their vehicle and tracked it for 28 days. *Id.* at 48. Ninety-one percent of participants responded that this violated their expectations of privacy, the highest of any of the 18 scenarios tested.[9] *Id.* at 47. Strikingly, the authors found privacy expectations in location tracking to be greater than in cases where the Court has instructed that a warrant is required, such as use of an infrared camera to peer inside a house, and even on par with physically searching a suspect's bedroom. *Id.* at 57. In contrast, nearly three times as many people found privacy vio-

---

[7] The researchers found somewhat lower expectations of privacy when they asked the question in the third person and specified that police found evidence of criminal activity. In that condition, an estimated 60% of people believed that obtaining cell site location information violated a person's reasonable expectation of privacy. Chao et al., *supra* p. 7, at 40-41, 44 Fig.1.

[8] Although the sample was not nationally representative, the authors reweighted the sample to more closely approximate the national population. Overall, the authors found that non-white participants had higher expectations of privacy in location data. The Chao et al. paper will appear later this year in the California Law Review. The results appear in a pre-publication version of the paper that is available here: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2924744.

[9] Again, the higher percentages here are attributed to the presumption of innocence embedded in the questions. As noted above in note 7, the percentages drop when respondents are told that authorities had pre-existing indicia of criminal behavior.

lations in location tracking than questioning at a roadblock.

Thus, nearly half of respondents in one study found the very fact of cell site and GPS data collection violative of privacy rights regardless of duration; the numbers increased substantially when scholars added a lengthy time component and told respondents to imagine an innocent target, as Fourth Amendment doctrine arguably requires.

A third study, which focused on real time surveillance, found that 60.6% of respondents agreed (33.3%) or strongly agreed (27.3%) that "[a]n individual has an expectation of privacy in the location data emitted from his or her cell phone" compared to only 14.4% who disagreed (11.5%) or strongly disagreed (2.9%). Alisa Smith, Sean Madden & Robert P. Barton, *An Empirical Examination of Societal Expectations of Privacy in the Digital Age of GPS, Cell Phone Towers, & Drones*, 26 Alb. L.J. Sci. & Tech. 111, 128, 133 (2016).

Finally, several studies probe people's views on actual law enforcement activities and duties, rather than their own views about what they hold private. When 1,195 individuals were asked to choose from a range of circumstances under which law enforcement should be able to access their "approximate past location information from cell phone tower signals," more than three-quarters of respondents selected a probable cause standard or higher (78.9%). Christine S. Scott-Hayward, Henry F. Fradella & Ryan G. Fischer, *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 Am. J. Crim. L. 19, 52–53 (2015–2016).[10] Respondents overwhelming-

---

[10] Participants were recruited through M-Turk and the sample was not nationally representative. Compared to the United

ly believed that law enforcement should either never be able to access this information (20.4%) or that they should have to demonstrate probable cause in order to access this information (58.5%). *Id.* Only 1.8% thought that the police should be able to access this data at any time without some level of process or suspicion. *Id.* Participants were also asked about their views on police access to location data derived from the GPS in their smartphones. Depending on the duration of tracking (one-time to two-to-four weeks), between 79.3% and 83.4% of participants thought that police officers should either have probable cause to access this information or that they should never be allowed to access it. Only 1.6–2.0% thought that it should be available without some level of process or suspicion. *Id.*

One of the studies previously mentioned replicates these results. When asked, 72.5% of respondents agreed (35.7%) or strongly agreed (36.8%) that "[t]he police must obtain a warrant, based on a showing of probable cause, from a judge to obtain tracking information through the use of a cell phone" compared to 9.6% who disagreed (6.8%) or strongly disagreed (2.8%). Smith et al., *supra* p. 8, at 128, 133. A similar question involving GPS tracking found that 66.7% of participants in their study agreed or strongly agreed that police should have to obtain a warrant before tracking a person for a month using a GPS device on their car. *Id.*

To be sure, these studies are varied in scope, approach and content, but they are uniformly transparent about their datasets and methods. And *all* of

---

States population, the sample included more males (56.7% compared with 49.2%), more Asians (9.6% compared with 4.8%), fewer Hispanics (8% compared with 16.3%) and fewer blacks (7.9% compared with 12.6%).

these studies reach the same result with respect to gathering historic cell site data without a warrant: it is deemed by average Americans to be highly unexpected, intrusive, or disturbing. No research suggests otherwise.

II. THE DATA ARE DOCTRINALLY SIGNIFICANT IN THIS COURT'S FOURTH AMENDMENT JURISPRUDENCE.

The empirical data set forth above can and should provide assistance to courts, including this Court, in assessing the scope and proper application of the Fourth Amendment.

First, this Court has generally accounted for the actual privacy expectations of ordinary Americans in many different Fourth Amendment contexts. *Smith*, 442 U.S. at 742–43 ("doubt[ing] that people in general entertain any actual expectation of privacy in the numbers they dial."); *California* v. *Ciraolo*, 476 U.S. 207, 213–14 (1986) (private property visible to the naked eye "is not [a privacy] expectation that society is prepared to honor."); *Minnesota* v. *Olson*, 495 U.S. 91, 98–99 (1990) ("To hold that an overnight guest has a legitimate expectation of privacy in his host's home merely recognizes the everyday expectations of privacy that we all share."); *Georgia* v. *Randolph*, 547 U.S. 103, 111 (2006) ("constant element in assessing Fourth Amendment reasonableness in the consent cases, then, is the great significance given to widely shared social expectations . . ."); *City of Ontario* v. *Quon*, 560 U.S. 746, 758–60 (2010) (noting that "the Court would have difficulty predicting how employees' privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable" in the context of work-issued pagers); *Florida* v. *Jardines*, 133 S. Ct. 1409, 1415–16 (2013) ("A license

may be implied from the habits of the country, notwithstanding the strict rule of the English common law as to entry upon a close.") (internal citation omitted). But cf. *United States* v. *Jacobsen*, 466 U.S. 109, 122–24 (1984) (emphasizing normative considerations rather than expectations in applying *Katz*).

What people expect and understand has consistently been a key consideration in search and seizure cases. *Rakas* v. *Illinois*, 439 U.S. 128, 143 n.12 (1978) (noting that "[l]egitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society."); see also *Kyllo* v. *United States*, 533 U.S. 27, 40 (2001) (suggesting that had the infrared surveillance technique at issue been in "general public use," such that people understood the infrared signature of one's house was routinely exposed passerby, then such surveillance would not have been a search); *United States* v. *Jones*, 565 U.S. 400, 408 (2012) ("[O]ur very definition of reasonable expectation of privacy [is one] which we have said to be an expectation that has a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society") (internal citation omitted). The principal alternative to examining ordinary people's actual expectations is for judges to rely exclusively on their own experiences and intuitions. But the American citizenry is poorer, more rural, less well-educated, and younger than the judiciary is, and those demographic differences can cause a mismatch in privacy expectations. See, *e.g.*, *Actual Expectations of Privacy*, *supra* note 5, at 255 (finding a statistically significant relationship between subject age and re-

ceptiveness to the third-party doctrine). Empirical research is a critical tool that grounds the *Katz* inquiry in reality rather than speculation.

Second, this Court routinely considers hard social science data in a variety of contexts, including the Fourth Amendment, to inform its decisionmaking. See, *e.g.*, *United States* v. *Leon*, 468 U.S. 897, 907 n.6 (1984) (relying on social science evidence to inform Court's decision not to apply exclusionary rule when officers relied in good faith on an invalid warrant); *Ballew* v. *Georgia*, 435 U.S. 223, 232–33 (1978) (jury deliberations); *In re Gault*, 387 U.S. 1, 20 n.26, 22 & 22 n.30 (1967) (due process in juvenile delinquency proceedings); *Brown* v. *Bd. of Educ. of Topeka*, 347 U.S. 483, 494–95 n.11 (1954) (effects of racial segregation); see also Shari Seidman Diamond & David J. Franklyn, *Trademark Surveys: An Undulating Path*, 92 Tex. L. Rev. 2029, 2030 (2014) (noting that many courts have considered surveys to be the "most direct form of evidence that can be offered on the consumer perception questions at issue in trademark and deceptive advertising litigation"). In the Fourth Amendment context, members of this Court and other jurists have noted that studies would be or are useful in assessing a person's reasonable expectations. See, *e.g.*, Transcript of Oral Argument at 43–44, *Brendlin* v. *California*, 551 U.S. 249 (2007) (No. 06-8120) (questions offered by Justice Breyer and Justice Scalia). Lower courts have already recognized its utility. See, *e.g.*, *Brandin* v. *State*, 669 So. 2d 280, 282 n.2 (Fla. Dist. Ct. App. 1996) (citing the Slobogin & Schumacher research); *Commonwealth* v. *Johnson*, 75 N.E.3d 51, 72 (Mass. Ct. App. 2017) (Wolohojian, J., dissenting) (citing the Kugler & Strahilevitz research); *Love* v. *State*, NO. AP-77,024, 2016 WL 7131259, at *6 (Tex. Ct. Crim. App. Dec. 7, 2016),

reh'g denied (Apr. 12, 2017) (citing the Scott-Hayward et al. research). The *Katz* test distinguishes between those forms of surveillance that are intrusive and unexpected, such that heightened procedural requirements are appropriate, and those that are minor inconveniences. An effective way to do that sorting is to use social science to identify which searches the public regards as most intrusive. Cf. Janice Nadler, *No Need to Shout: Bus Sweeps and the Psychology of Coercion*, 2002 Sup. Ct. Rev. 153, 201 (2002) (noting that "[t]he simplest way to determine whether a reasonable person voluntarily consented to a police search is simply to ask them, 'To what extent did you feel free to decline the officer's request?'").

Given courts' routine resort to these kinds of data, scholars who contend that such social science evidence is beyond judicial comprehension or unreliable are mistaken. See, *e.g.*, Orin S. Kerr, *Do We Need a New Fourth Amendment?*, 107 Mich. L. Rev. 951, 964–66 (2009). Such critiques address the first generation of empirical research, which relied exclusively on small sample sizes or convenience samples of college student respondents, and subsequent research has addressed their criticisms or shown their worries about the data to be overblown. See, *e.g.*, Christopher Slobogin, *Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire*, 94 Minn. L. Rev. 1588, 1594–1604 (2009–2010); *Actual Expectations of Privacy*, *supra* note 5, at 231–35. And to the extent that these scholars believe the data to be aspirational or inconsistent, the authors amply demonstrated above that notwithstanding differences among samples and questions, popular sentiment coalesced in a consistent way in supporting a reasonable expectation of privacy in cell site location information. When multiple, well-designed, published, and replicated so-

cial science studies confirm that most Americans expect privacy in a given context, holding that an expectation of privacy presumptively exists under *Katz* would render Fourth Amendment law clearer and more predictable.

Recent research also answers two other common critiques. First is the concern that survey participants may think that any type of law enforcement action is highly intrusive. But that is not the case. See, *e.g.*, Chao et al., *supra* p. 7, at 47–48 tbl.2 (showing that people view brief questioning at police roadblocks and the use of automated gunshot detecting microphones in public places as relatively noninvasive); *Actual Expectations of Privacy*, *supra* note 5, at 260 tbl.9 (showing that people view cameras in parks and use of facial recognition technology at sporting events as fairly non-intrusive); Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* 183–84 (2007) ("*Privacy at Risk*") (showing that techniques like the use of roadblocks, obtaining airplane passenger manifests, or getting traffic and criminal records, are not deemed particularly intrusive). Participants are therefore distinguishing between different types of searches, and not reflexively demanding privacy.

Second, both this Court and scholars have worried that the public's Fourth Amendment expectations may depend in part on what this Court pronounces them to be, creating circularity. See, *e.g.*, *Kyllo*, 533 U.S. at 34; Erwin Chemerinsky, *Rediscovering Brandeis's Right to Privacy*, 45 Brandeis L.J. 643, 650 (2006–2007); Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 Sup. Ct. Rev. 173, 188 (1979). Yet new data suggest that the public does not alter its beliefs about Fourth Amendment protections even in the wake of well-

publicized and unanimous Supreme Court decisions that alter search and seizure law. One study conducted nationally representative surveys on four occasions to measure privacy expectations incident to arrest before and after the decision in *Riley* v. *California*, 573 U.S. __ (2014). Despite *Riley*'s strong language and holding in support of cell phone privacy, privacy expectations on that point moved only very slightly two weeks after the decision and had returned to baseline when measured one and two years later. Matthew B. Kugler & Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U. Chi. L. Rev. (forthcoming 2017).[11] Based on this research, there is ample reason to believe the public's actual expectations of privacy are stable over time and rather impervious to changes in the law.[12]

For more than twenty-five years scholars have suggested specific ways that reliable social science data can be incorporated into this Court's *Katz* test. Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 Duke L.J. 727, 732 (1993). The scholarship identifies

---

[11] The empirical results of this forthcoming article have been finalized. A draft containing those results appears at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2922777.

[12] Our approach still leaves room for normative considerations. As this Court has previously recognized, a normative rather than empirical inquiry would be proper if "an individual's subjective expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms." *Smith*, 442 U.S. at 740 n.5. Further, even if this Court finds a given activity to be a search for Fourth Amendment purposes, it would still need to decide if that search is "reasonable" without a warrant.

several doctrinal hooks for incorporating such data, ranging from a proportionality test, to a resuscitated *Katz* prong 1 test, to incorporating the data into *Katz*'s prong 2 analysis. See *Privacy at Risk*, *supra* p. 14, at 33–39; *Actual Expectations of Privacy*, *supra* note 5, at 223–24, 240–44; Scott-Hayward et al., *supra* p. 8, at 49. Regardless of precisely where such data fit into the *Katz* test, it should be clear that when multiple reputable studies using divergent methods all agree that most Americans regard cell site location information as private and sensitive, courts should take these privacy expectations into account.

CONCLUSION

For the foregoing reasons, this Court should reverse the Sixth Circuit.

Respectfully submitted,

SARAH O'ROURKE SCHRUP *
JEFFREY T. GREEN
NORTHWESTERN SUPREME COURT PRACTICUM
375 East Chicago Avenue
Chicago, IL 60611
(312) 503-0063
s-schrup@law.northwestern.edu

Counsel for Amici Curiae

August 14, 2017

* Counsel of Record

APPENDIX

APPENDIX

Amici Curiae

Bernard Chao

Bernard Chao is an Associate Professor at the University of Denver Sturm College of Law and co-director of the Denver Empirical Justice Institute. He teaches patent, intellectual property and privacy law. Beyond research in these fields, his papers also address cognitive bias in legal decision-making.

Ian Farrell

Ian Farrell is an Associate Professor at the University of Denver Sturm College of Law. He teaches criminal procedure, criminal law, and constitutional law, among other subjects. His research has been published in the Texas Law Review, the Boston College Law Review, the William and Mary Law Journal, and elsewhere.

Ryan G. Fischer, Ph.D.

Ryan G. Fischer is an Associate Professor in the School of Criminology, Criminal Justice, and Emergency Management at California State University, Long Beach. He continually collaborates with colleagues with social science and legal expertise to provide methodological and statistical contributions to research studies. He has contributed to multiple research articles aimed at examining the importance of providing empirical research findings to better inform legal decision making. These articles have been pub-

lished in both law reviews and peer-reviewed social science journals.

Henry F. Fradella, Ph.D.

Henry F. Fradella, is a Professor in, and Associate Director of, the School of Criminology and Criminal Justice at Arizona State University. He researches substantive and procedural criminal law; the dynamics of legal decision-making; and the nature, sources, and consequences of variations and changes in legal institutions or processes. A fellow and past-president of the Western Society of Criminology, Dr. Fradella is the author or co-author of 10 books and more than 80 articles, book chapters, reviews, and scholarly commentaries that have been published in both law reviews and peer-reviewed social science journals.

Chris Jay Hoofnagle

Chris Jay Hoofnagle is adjunct full professor of Information and of Law at the University of California, Berkeley, where he has taught computer crime law, internet law, privacy law, and courses on security and privacy technology. With colleagues, he has written several reports on privacy attitudes based on nationwide, telephonic surveys.

Matthew B. Kugler, Ph.D.

Matthew B. Kugler is an Assistant Professor of Law at Northwestern Pritzker School of Law. He has written extensively on privacy and Fourth Amendment issues. He teaches privacy law and intellectual property.

J.J. Prescott, Ph.D.

J.J. Prescott is a Professor of Law at the University of Michigan Law School, co-directs Michigan's Program in Law and Economics and its Empirical Legal Studies Center, and has appointments in Michigan's Economics Department and Population Studies Center. Professor Prescott has a PhD on economics from MIT, teaches and writes in the area of criminal law and procedure, and has published empirical research in both law reviews and peer-reviewed social science journals.

Christopher Robertson

Christopher Robertson is Professor and Associate Dean at the University of Arizona James E. Rogers College of Law. His empirical research has been published in New England Journal of Medicine, Journal of Legal Analysis, Journal of Empirical Legal Studies, and elsewhere.

Christopher Slobogin

Christopher Slobogin occupies the Milton Underwood Chair at Vanderbilt University Law School. His publications on the Fourth Amendment include a University of Chicago Press book and articles in the Duke, Minnesota, UCLA, and University of Chicago law reviews. He is the recipient of Distinguished Contribution Awards from the two leading forensic psychology organizations specializing in empirical work and an Associate Reporter for the American Law Institute's Principles of Policing Project.

Christine Scott-Hayward, Ph.D.

Christine Scott-Hayward is an Assistant Professor in the School of Criminology, Criminal Justice, and Emergency Management at California State University, Long Beach. She researches and teaches broadly in the areas of courts and criminal procedure and is the author or co-author of numerous articles published in both law reviews and peer-reviewed social science journals.

Alisa Smith, Ph.D.

Alisa Smith is an Associate Professor of Legal Studies at the University of Central Florida. Her scholarship and teaching has focused on the empirical study of the Fourth Amendment and the criminal courts.

Sonja Starr

Sonja Starr is Professor of Law and Co-Director of the Empirical Legal Studies Center at the University of Michigan. Her research employs both quantitative empirical methods and doctrinal analysis, and focuses on policing, sentencing, and prisoner reentry. Her recent work is published or forthcoming in the Quarterly Journal of Economics, the Journal of Political Economy, the American Law and Economics Review, the Yale Law Journal, and the Stanford Law Review."

Lior Strahilevitz

Lior Strahilevitz is the Sidley Austin Professor of Law at the University of Chicago, where he teaches privacy law. Professor Strahilevitz has published articles on privacy and/or criminal procedure in the Harvard Law Review, the University of Chicago Law Review, the California Law Review, the Northwestern University Law Review, the NYU Law Review, the Supreme Court Review, and the Journal of Legal Studies. Professor Strahilevitz is an Adviser to the American Law Institute's Principles of Law, Data Privacy Project.

Matthew Tokson

Matthew Tokson is an Associate Professor at the University of Utah, S.J. Quinney College of Law. He has written several articles about the Fourth Amendment, civil privacy law, internet law, and new technologies. His most recent article appeared in the Northwestern University Law Review and won peer-judged awards for excellence from the Privacy Law Scholars Conference and the Southeastern Association of Law Schools Conference. He teaches criminal procedure and cyberlaw, among other subjects.

Jennifer M. Urban

Jennifer M. Urban is a clinical professor of law at the University of California, Berkeley. Her research and teaching include privacy, security, consumer interests, and civil liberties. Together with co-authors, she has published empirical work on Americans' understanding of and attitudes toward privacy issues.

RECORD AND BRIEF

No. 16-402

FILED
2017
OFFICE OF THE CLERK

In The
Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ Of Certiorari To The United States Court Of Appeals For The Sixth Circuit

BRIEF OF INSTITUTE FOR JUSTICE, CAROLE HINDERS, RANDY AND KAREN SOWERS, AND DKT LIBERTY PROJECT AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

INSTITUTE FOR JUSTICE
WESLEY HOTTOT*
10500 Northeast 8th Street,
Suite 1760
Bellevue, WA 98004
Tel: (425) 646-9300
E-mail: whottot@ij.org

ROBERT P. FROMMER
901 North Glebe Road, Suite 900
Arlington, VA 22203
Tel: (703) 682-9320
E-mail: rfrommer@ij.org

**Counsel of Record*

Counsel for Amici Curiae

COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES iii

INTEREST OF THE *AMICI CURIAE* 1

SUMMARY OF ARGUMENT 3

ARGUMENT 6

I. In Answering the Question Presented, This Court Should Be Mindful of How Its Decision in *United States v. Miller* Has Negatively Impacted Ordinary Americans 6

A. *Miller* adopted a categorical approach to the Third Party Doctrine that has transformed the Bank Secrecy Act into a general warrant for federal agents to monitor people's bank accounts 7

B. Federal agents now routinely surveil the everyday banking practices of ordinary Americans looking for property to forfeit 11

C. As a result of *Miller*, even people who have done nothing wrong – people like *amici* – are finding themselves targeted for civil forfeiture without being charged with a crime 14

1. The Internal Revenue Service used the categorical approach to the Third Party Doctrine to monitor Carole Hinders' bank account and wrongfully seize more than $32,000 17

TABLE OF CONTENTS – Continued

Page

2. Randy and Karen Sowers received the same treatment and had more than $62,000 wrongfully seized 23

II. This Court Should Reject the Categorical Approach to the Third Party Doctrine 26

A. Applying the categorical approach of *Miller* to the cell-site-location information in this case would lead to the same dragnet surveillance of phone information that the nation has experienced in banking 27

B. The Court should reject the categorical approach to the Third Party Doctrine and instead adopt a real-world approach that scrutinizes positive law, including statutes and private contracts 34

CONCLUSION 37

TABLE OF AUTHORITIES

Page

CASES

California Bankers Assoc. v. Shultz, 416 U.S. 21 (1974) 7

In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747 (S.D. Tex. 2005) 29

Katz v. United States, 389 U.S. 347 (1967) 9

Leonard v. Texas, 137 S. Ct. 847 (2017) 12, 13

Riley v. California, 134 S. Ct. 2473 (2014) 2

SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735 (1984) 10

Smith v. Maryland, 442 U.S. 735 (1979) 7, 8, 34

United States v. Funds in the Amount of $30,670, 403 F.3d 448 (7th Cir. 2005) 32

United States v. $32,820.56 in U.S. Currency, 838 F.3d 930 (8th Cir. 2016) 22

United States v. $32,820.56 in U.S. Currency, 106 F. Supp. 3d 990 (N.D. Iowa 2015) 22

United States v. $32,820.56 in U.S. Currency, 79 F. Supp. 3d 927 (N.D. Iowa 2015) 22

United States v. $32,820.56 in U.S. Currency, No. C13-4102-LTS (N.D. Iowa filed Oct. 24, 2013) 19, 20

United States v. $33,244.86 in U.S. Currency from TCF Nat'l Bank Account #XXXXXX6598, No. 2:13-cv-13990-RHC-DRG (E.D. Mich. filed Sept. 18, 2013) 15

TABLE OF AUTHORITIES – Continued

Page

United States v. $35,651.11 in U.S. Currency Seized from PNC Account No. XXXXXX6937, No. 4:13-cv-13118 (E.D. Mich. filed July 19, 2013) 15

United States v. $107,702.66 in U.S. Currency Seized from Lumbee Guaranty Bank, Account No. XXXX2495, No. 7:14-cv-00295-F (E.D.N.C. filed Dec. 23, 2014) 15

United States v. $174,206.00 in U.S. Currency, 320 F.3d 658 (6th Cir. 2003) 32

United States v. Jones, 565 U.S. 400 (2012) 27, 29

United States v. MacPherson, 424 F.3d 183 (2d Cir. 2005) 14, 19

United States v. Miller, 425 U.S. 435 (1976) ..... *passim*

United States v. Sperrazza, 804 F.3d 1113 (11th Cir. 2015) 14

United States v. Sturman, 951 F.2d 1466 (6th Cir. 1991) 9

United States v. Sweeney, 611 F.3d 459 (8th Cir. 2010) 19

United States v. Van Allen, 524 F.3d 814 (7th Cir. 2008) 19

CONSTITUTIONAL PROVISIONS

U.S. Const. amend. IV ..... *passim*

TABLE OF AUTHORITIES – Continued

Page

STATUTES

12 U.S.C. § 1829b(d) 8, 14

18 U.S.C. § 981(c) 12

18 U.S.C. § 984(a)(2) 15

18 U.S.C. § 2703 30

28 U.S.C. § 2465(b)(1) 22

31 U.S.C. § 5317(c) 15

31 U.S.C. § 5318(g) 10

31 U.S.C. § 5324(a) 14

47 U.S.C. § 222(f) 36

12 C.F.R. § 21.11 10

31 C.F.R. § 1010.100(xx) 14

31 C.F.R. § 1010.311 14

OTHER PUBLICATIONS

William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv. L. Rev. 1821 (2016) 35

Bureau of Labor Statistics, U.S. Dep't of Labor, CPI Inflation Calculator, https://data.bls.gov/cgi-bin/cpicalc.pl 15

TABLE OF AUTHORITIES – Continued

Page

Congress must end abuses of seizures by feds, Des Moines Register, Nov. 8, 2014, www.desmoinesregister.com/story/opinion/editorials/2014/11/08/congress-must-stop-seizures/18728827/ 21

Daniel P. Finney, *Forfeiture target calls it, 'a violation of civil rights'*, Des Moines Register, Nov. 2, 2014, www.desmoinesregister.com/story/news/crime-and-courts/2014/11/02/civil-forfeiture-iowa-carole-hinders-arnolds-park/18362299/ 21

Eric Holder, Memorandum, *Guidance Regarding the Use of Asset Forfeiture Authorities in Connection with Structuring Offenses* (Mar. 31, 2015), www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/31/ag-memo-structuring-policy-directive.pdf 22

Institute for Justice, D. Carpenter, L. Knepper, A. Erickson, J. McDonald, *Policing for Profit: The Abuse of Civil Asset Forfeiture* (2d ed. Nov. 2015), http://ij.org/report/policing-for-profit/ 12, 31

Institute for Justice, D. Carpenter & L. Salzman, *Seize First, Question Later: The IRS and Civil Forfeiture* (Feb. 2015), http://ij.org/wp-content/uploads/2015/03/seize-first-question-later.pdf 15

Internal Revenue Service, U.S. Dep't of Treasury, Memorandum for Special Agents in Charge: IRS Structuring Investigation Policy Changes (Oct. 17, 2014), *available at* http://ij.org/wp-content/uploads/2015/07/IJ068495.pdf 21

TABLE OF AUTHORITIES – Continued

Page

Richard M. Re, *The Positive Law Floor: Responding to William Baude & James Y. Stern, The Positive Law Model of the Fourth Amendment*, 129 Harv. L. Rev. F. 313 (2016) 36

Jennifer Shasky Calvery, Address at the FinCEN 2015 Law Enforcement Awards Ceremony, May 12, 2015, https://www.fincen.gov/sites/default/files/2016-08/20150512.pdf 11

Petition for Remission or Mitigation of Randy and Karen Sowers (July 16, 2015), http://ij.org/wp-content/uploads/2015/07/irs-forfeiture-petitions-randy-sowers-petition.pdf 25

Sarah N. Welling, *Smurfs, Money Laundering and the Federal Criminal Law: The Crime of Structuring Transactions*, 41 Fla. L. Rev. 287 (1989) 11, 14

Shaila Dewan, *Law Lets I.R.S. Seize Accounts on Suspicion, No Crime Required*, N.Y. Times, Oct. 26, 2014, at A1, http://www.nytimes.com/2014/10/26/us/law-lets-irs-seize-accounts-on-suspicion-no-crime-required.html 20

Statement of Richard Weber, Chief of I.R.S. Criminal Investigation, N.Y. Times, Oct. 25, 2014, www.nytimes.com/2014/10/26/us/statement-of-richard-weber-chief-of-irs-criminal-investigation.html 21

TABLE OF AUTHORITIES – Continued

Page

Thieves in Suits, Richmond Times-Dispatch, Oct. 29, 2014, www.richmond.com/opinion/our-opinion/editorial-thieves-in-suits/article_aaac41c4-8e8c-5db5-9a8f-c1e67790b7fd.html 20

Treasury Inspector General for Tax Administration, *Criminal Investigation Enforced Structuring Laws Primarily Against Legal Source Funds and Compromised the Rights of Some Individuals and Businesses*, Ref. No. 2013-30-025 (Mar. 30, 2017), www.treasury.gov/tigta/auditreports/2017reports/201730025fr.pdf 16, 17

U.S. GAO Report, Bank Secrecy Act: Increased Use of Exemption Provisions Could Reduce Currency Transaction Reporting While Maintaining Usefulness to Law Enforcement Efforts, GAO-08-355 (Feb. 2008), http://www.gao.gov/assets/280/272447.pdf 13

United States' Combined Br. & Resp. to Defs.' Mots. in Limine, Ex. 2, *United States v. Carpenter*, No. 2:12-cr-20218-SFC-MKM-4 (E.D. Mich. filed Dec. 24, 2013), ECF No. 221-2 30

When the Government Charges Your Property With a Crime, Not You, Iowa Public Radio, Nov. 5, 2014, iowapublicradio.org/post/when-government-charges-your-property-crime-not-you#stream/0 20

INTEREST OF THE *AMICI CURIAE*[1]

The Institute for Justice is a nonprofit, public-interest law firm dedicated to defending the essential foundations of a free society, including property rights and the Fourth Amendment right to be free from warrantless government surveillance.

Three of the *amici* – Carole Hinders and Randy and Karen Sowers – are Institute for Justice clients from whom the Internal Revenue Service (IRS) wrongfully seized over $90,000. In their cases, the government relied on the Third Party Doctrine to scrutinize *amici*'s banking habits without a warrant, and so intruded on the details of *amici*'s daily lives without establishing probable cause before a neutral magistrate. In both cases, the government used this sweeping surveillance power to identify a pattern of less than $10,000 cash deposits, which, according to one IRS agent, rose to the level of "structuring" in violation of federal bank reporting laws. (A thorough investigation would have revealed that *amici* ran small businesses that relied on cash and made frequent deposits below $10,000.) *Amici* were not charged with "structuring" or any other crime. Even so, the categorical approach to the Third Party Doctrine made it possible for the government to secretly review their bank records and wrongfully seize their accounts. Using civil forfeiture,

---

[1] All parties have consented to the filing of this brief. *Amici* affirm that no counsel for any party authored this brief in whole or in part and that no person or entity made a monetary contribution specifically for the preparation or submission of this brief.

the government forced *amici* to litigate, at their own expense, for the return of their money. And, because the federal government keeps 100% of property it successfully forfeits, the IRS had a direct profit incentive in those proceedings. *Amici* fought back and, with the Institute for Justice representing them pro bono, their money was eventually returned – 21 months later in Carole's case and four years later in Randy and Karen's case.

What happened to Carole, Randy, and Karen was only possible because, under this Court's precedents, information a person conveys to a bank is categorically excluded from Fourth Amendment protection. If the same categorical rule were applied to the cell-site-location information (CSLI) at issue in this case, innocent Americans would be caught up in dragnet searches of their CSLI, just as Carole, Randy, and Karen were caught up in dragnet searches of their bank records. It is *amici*'s hope that their experiences will lead the Court to reject the categorical approach to the Third Party Doctrine and, instead, apply a real-world approach. Specifically, in determining whether CSLI requires Fourth Amendment reasonableness analysis (and, ultimately, a warrant), *amici* urge the Court to take account of the privacy protections available to private parties under statutes and contracts.

Amicus DKT Liberty Project is a nonprofit dedicated to promoting individual liberty and defending the right to privacy. Founded in 1997, the Liberty Project has participated as *amicus* in this Court several

times, including in *Riley v. California*, 134 S. Ct. 2473 (2014). Like *Riley*, this case concerns the privacy of information generated by Americans' cell phones – their modern day papers and effects. The smartphone is a computer, creating and holding countless private papers, and potentially providing government with a trove of information about a person, their home, business, and family members. Because of the Liberty Project's experience protecting Americans' privacy from government overreach, it is well situated to provide this Court with additional insight into the question presented in this case.

SUMMARY OF ARGUMENT

This case is about the intersection of cutting edge technology and the Fourth Amendment, so it is understandable that the parties are focused on the future of CSLI. In deciding that important future, however, *amici* urge this Court to be mindful of the past.

This brief explains why the categorical approach to the Third Party Doctrine announced in *United States v. Miller* is a poor foundation on which to build the Fourth Amendment's future. *Miller* categorically exempted from Fourth Amendment protection *any* information a person provides to their bank, under *any* circumstances. In the 41 years since, this categorical reasoning has given law enforcement license to monitor virtually every bank account in the country looking for suspicious activity. Technological advances have

made possible ever-more comprehensive bank surveillance so that, today, the federal government collects at least 12 times more bank information *every day* as it collected in an *entire year* when *Miller* was decided. All of this surveillance occurs with zero judicial oversight.

At the same time, civil forfeiture has metastasized from a legal backwater into a favored tool of law enforcement – a tool that has combined with the categorical approach to the Third Party Doctrine to endanger the rights of ordinary Americans. Law enforcement has come to rely on civil forfeiture because it allows them to take property without charging (let alone convicting) anyone with a crime. And, because federal agencies keep 100% of the proceeds of everything they forfeit, they have a direct financial incentive to seize more and more property. While *Miller* has given the government the *means* to monitor Americans' banking practices, the profit incentive to pursue civil forfeiture has provided a powerful *motive* to do so. As a result, federal agents now troll Americans' banking information looking for property they can seize, putting the burden on property owners to fight back at their own expense.

As *amici*'s experiences show, the federal government uses this power to devastating effect. Take for instance *amici* Carole Hinders and Randy and Karen Sowers, who endured civil forfeiture nightmares based on innocent banking behavior. Under *Miller*, the government was able to secretly monitor *amici*'s bank records. Based on a cursory review of those records, the

government seized their bank accounts without any criminal charges. In the end, *amici* were successful in getting their money back, but it took more than 21 months in Carole's case and more than four years in the Sowers' case. And their experiences are far from unique.

Thus, what the Court envisioned – in *Miller* – as the piecemeal collection of bank records for criminal prosecutions has become a nationwide surveillance program devoted in substantial part to civil forfeiture actions. This unanticipated expansion of *Miller* should give this Court pause as it considers what Fourth Amendment rule to apply to CSLI.

Amici urge the Court to reject the categorical approach to the Third Party Doctrine. Applied to the CSLI at issue in this case, the categorical approach would result in the same type of dragnet surveillance the nation has experienced in the banking context. This outcome would only add fuel to the government's already out-of-control forfeiture machine. Like bank information collected without a warrant, CSLI can – and would – be used to justify civil forfeiture proceedings against innocent people.

In place of the categorical approach, the Court should adopt a real-world approach to the Third Party Doctrine that uses predictable standards derived from positive law. This approach would weigh the statutes and private contracts that restrain a private person's access to information that the government seeks to obtain without a warrant. Fourth Amendment

reasonableness standards would govern whenever a private person would violate the law by obtaining the same information without the suspect's consent. Rather than giving the government blanket license to collect and troll the CSLI of every American, this approach would interpose judicial checks and balances based on predictable standards

ARGUMENT

I. In Answering the Question Presented, This Court Should Be Mindful of How Its Decision in *United States v. Miller* Has Negatively Impacted Ordinary Americans.

The question presented asks whether the warrantless search of CSLI is permissible under the Fourth Amendment. *See* Brief for Petitioner at i. When this Court answered a similar question 41 years ago in the banking context, it applied a categorical rule, holding that defendants have no reasonable expectation of privacy in personal information that they shared with their banks, regardless of any private agreements that required the bank to keep such information confidential. *United States v. Miller*, 425 U.S. 435, 445 (1976). Then, as now, banks were required to collect vast amounts of information about their customers and convey it to the government under the Bank Secrecy Act.[2]

[2] Shortly before *Miller*, this Court upheld the constitutionality of the Bank Secrecy Act, holding that banks can be required to

Miller has made it possible for the government to systematically collect this information – and more – without any judicial determination of probable cause to believe a crime has been committed. As *amici*'s experiences show, federal agents use this power to troll Americans' bank records for property that can be forfeited. This has led to innocent people – people like *amici* – being swept up in civil forfeiture proceedings in which they are never charged with, let alone convicted of, a crime.

The past is prologue: The troubling expansion of the Third Party Doctrine under *Miller* cautions against using similar categorical reasoning in this case.

A. *Miller* adopted a categorical approach to the Third Party Doctrine that has transformed the Bank Secrecy Act into a general warrant for federal agents to monitor people's bank accounts.

Amici agree with Petitioner that the bank records in *Miller* and the telephone numbers in *Smith v. Maryland*, 442 U.S. 735 (1979), offer a poor basis for comparison to the CSLI at issue in this case. *See* Brief for Petitioner at 35-47. This brief seeks to make an additional point: The categorical approach to the Third Party Doctrine adopted in *Miller* (and applied in *Smith*) has led to innocent people being swept up in dragnet searches of their banking practices. Although

---

collect information about their customers. *See California Bankers Assoc. v. Shultz*, 416 U.S. 21 (1974).

Miller and *Smith* involved criminal prosecutions, law enforcement now uses the sweeping authority of the Third Party Doctrine as a tool to seize and take legal possession of people's property through civil forfeiture, often with no criminal charges.

Like this case, *Miller* involved a criminal defendant – a man suspected of operating an illegal whiskey distillery. *See* 425 U.S. at 436. After a fire broke out in a warehouse he rented, local police discovered a large whiskey operation there. *Id.* at 437. Federal authorities took over the investigation and built their case, in part, by subpoenaing two banks Miller had used – demanding copies of his checks, deposit slips, and financial statements. *Id.* at 437-38. At the time, banks were required to keep this information (just as they are today) under the Bank Secrecy Act, 12 U.S.C. § 1829b(d). 425 U.S. at 440-41. Miller's bank records provided the government with "one or two" leads in the investigation and, at trial, several checks were introduced to demonstrate a conspiracy to defraud the United States of whiskey taxes. *See id.* at 436, 438.

After a jury convicted him, Miller appealed, arguing that before the government could constitutionally obtain records from his bank, agents needed a warrant signed by a judge – not just a subpoena. This Court rejected that argument, holding "there was no intrusion into any area in which [Miller] had a protected Fourth Amendment interest." *Id.* at 440. The Court reasoned that the records "contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," and that,

therefore, Miller had "take[n] the risk, in revealing his affairs to another, that the information w[ould] be conveyed by that person to the Government." *Id.* at 442-43. The Court also rejected Miller's argument, based on *Katz v. United States*, 389 U.S. 347, 353 (1967), that he had a "reasonable expectation of privacy" in his bank records because "they [were] merely copies of personal records that were made available to the banks for a limited purpose." 425 U.S. at 442. The Court explained it had "held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, *even if the information is revealed on the assumption that it will be used only for a limited purpose*." *Id.* at 443 (emphasis added).

This last phrase, in particular, has cemented the current approach to the Third Party Doctrine in place, making it resistant to change in an era of rapid technological advancement. By excluding from Fourth Amendment protection even information that two private parties have contractually agreed to keep confidential, *Miller* has made it impossible for banks to offer greater privacy, leaving no way for expectations of privacy to change over time. Banks are, in fact, legally prohibited from offering their customers any privacy against warrantless government surveillance. Agreements to the contrary would only be misleading: No bank can provide a meaningful shield against the broad subpoena power of U.S. law enforcement under *Miller*. *See, e.g.*, *United States v. Sturman*, 951 F.2d 1466, 1483-84 (6th Cir. 1991) (holding that, despite

stronger privacy protections available in Switzerland, records of a Swiss bank could be secretly subpoenaed without invading the depositor's Fourth Amendment rights). Indeed, under this Court's precedents, people have no right to *know* that the government has required their bank to hand over financial information. *See SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) (holding that the targets of subpoenas have no Fourth Amendment right to notification when their banks are served). Even without a subpoena, banks are legally required to report "suspicious" activity and prohibited from notifying customers about the report. 31 U.S.C. § 5318(g); 12 C.F.R. § 21.11. As a result, there is no way to "opt out" of this massive surveillance program.

Thus, while *Miller* involved subpoenas issued by a United States Attorney, today a bank would almost certainly deliver the same information to the government as a matter of course, under the Bank Secrecy Act. Even when banks *are* subpoenaed, there is no judicial scrutiny of any kind. No proof of a crime is necessary. No threshold standard of proof needs to be satisfied. Mere "suspicion" is enough, whether on the part of a government agent or a single bank teller. As the next two sections show, federal authorities make full use of this sweeping power to secretly review people's banking information, to disastrous effect for innocent property owners like Carole Hinders and Randy and Karen Sowers.

B. Federal agents now routinely surveil the everyday banking practices of ordinary Americans looking for property to forfeit.

When *Miller* was decided in 1976, as a practical matter, the government could not obtain anything like a comprehensive view of Americans' bank records. The year before, in 1975, banks filed a mere 3,418 currency transaction reports, in which they disclosed suspicious banking behavior to the Treasury Department. *See* Sarah N. Welling, *Smurfs, Money Laundering, and the Federal Criminal Law: The Crime of Structuring Transactions*, 41 Fla. L. Rev. 287, 295 n.39 (1989). Contrast that with the present: In 2014, banks filed more than *15 million* currency transaction reports – over 41,000 each day – according to the director of the Treasury Department's Financial Crimes Enforcement Network (FinCEN). Jennifer Shasky Calvery, Address at the FinCEN 2015 Law Enforcement Awards Ceremony, at 2, May 12, 2015, https://www.fincen.gov/sites/default/files/2016-08/20150512.pdf. In other words, there are 12 times more currency transaction reports filed in a *single day* now than in the *entire year* before *Miller* was decided. And FinCEN has granted "more than 10,000 agents, analysts, and investigative personnel from over 350 unique agencies across the U.S. Government [] direct access to the reporting," the director noted. *Id.* at 4. As a result of technological advances, these thousands of agents, across hundreds of agencies, can now comprehensively review this trove of information

based on their own initiative, without a warrant or even a subpoena.

While the Third Party Doctrine provides law enforcement with the means to review troves of banking data, civil forfeiture provides a powerful financial incentive to do so. As one member of this Court recently observed, civil forfeiture has become "highly profitable." *Leonard v. Texas*, 137 S. Ct. 847, 848 (2017) (Thomas, J., statement respecting denial of certiorari). Indeed, like law enforcement agencies in many states, federal agencies either keep property they forfeit or keep 100% of the proceeds. *See* 18 U.S.C. § 981(e). This has led to an explosion of forfeiture activity. The year the Department of Justice's Assets Forfeiture Fund was established, in 1986, it took in just $93.7 *million* in deposits. *See* Institute for Justice, D. Carpenter, L. Knepper, A. Erickson, J. McDonald, *Policing for Profit: The Abuse of Civil Asset Forfeiture* (2d ed. Nov. 2015), at 10, http://ij.org/report/policing-for-profit/. By 2014, annual deposits had increased 4,667% to $4.5 *billion*. *Id.* Much of this increase occurred in the last decade and a half: From 2001 to 2014, the Justice and Treasury departments deposited $29 billion in forfeiture funds, an increase of more than 1,000% over that 13-year period.[3] *Id.* As Justice Thomas observed: "This

[3] Net assets in the Justice and Treasury department's forfeiture accounts – the amount of money retained after paying various obligations – increased 485% between 2001 and 2014. Institute for Justice, *Policing for Profit*, at 10. Net assets topped $1 billion for the first time in 2007 and ballooned to nearly $4.5 billion by 2014. *Id.*

system – where police seize property with limited judicial oversight and retain it for their own use – has led to egregious and well-chronicled abuses." *Leonard*, 137 S. Ct. at 848. The injustice of allowing agencies to profit from forfeitures is only compounded by the fact that "forfeiture operations frequently target the poor and other groups least able to defend their interests in forfeiture proceedings." *Id.*

Not surprisingly, the staggering collection of data authorized in *Miller* has contributed to the explosion of forfeiture activity. In 2008, the Government Accountability Office surveyed local and state agencies with access to currency transaction report data. More than half said the reports "identified assets that were previously unknown, including those that could be used for forfeiture action." U.S. GAO Report, Bank Secrecy Act: Increased Use of Exemption Provisions Could Reduce Currency Transaction Reporting While Maintaining Usefulness to Law Enforcement Efforts, GAO-08-355 (Feb. 2008), at 20, http://www.gao.gov/assets/280/272447.pdf. With virtually limitless data at their fingertips and a strong incentive to find forfeiture dollars, police and prosecutors have every reason to search for more forfeiture cases.

As the next section demonstrates, this is exactly what federal authorities have done: They use the staggering amount of banking information available under *Miller* to look for opportunities to seize money from people, many of whom have done nothing wrong.

C. As a result of *Miller*, even people who have done nothing wrong – people like *amici* – are finding themselves targeted for civil forfeiture without being charged with a crime.

Although *Miller* involved a criminal defendant, the categorical rule that it announced now impacts even ordinary people who have done nothing wrong. The cases of Carole Hinders and Randy and Karen Sowers illustrate this troubling development.

Their cases involved an obscure federal crime known as "structuring," although Carole, Randy, and Karen were never charged with that crime (or any other crime). Just as forfeiture activity was exploding, in 1986, Congress passed the structuring law in an effort to prevent people from circumventing banks' reporting obligations under the Bank Secrecy Act. *See United States v. MacPherson*, 424 F.3d 183, 188-89 (2d Cir. 2005) (discussing purpose of the structuring laws); *United States v. Sperrazza*, 804 F.3d 1113, 1130-33 (11th Cir. 2015) (Rosenbaum, J., dissenting) (collecting legislative history). Specifically, banks are required to file currency transaction reports for all cash transactions over $10,000, and the structuring law and Treasury regulations make it unlawful to purposefully evade this reporting threshold. *See* 31 U.S.C. § 5324(a) (defining the crime of structuring); 31 C.F.R. § 1010.100(xx) (same); 31 C.F.R. § 1010.311 (setting $10,000 threshold). The reporting threshold has remained unchanged since it was put in place in 1970, *see* Welling, 41 Fla. L. Rev. at 292-93, although an inflation-adjusted figure

would now exceed $60,000.[4] Increasingly, these laws have been deployed against people accused of nothing more than doing business in cash and depositing their money in the bank in a manner that the government deems "suspicious."[5]

This is possible because, in addition to criminal penalties, "structured" deposits (and funds commingled with those deposits) are subject to civil forfeiture. *See* 31 U.S.C. § 5317(c); 18 U.S.C. § 984(a)(2). The power of federal agencies to civilly forfeit property and keep the proceeds, combined with unfettered access to bank records, has given the government both the means and the motive to seize cash from legitimate businesses.

And that is exactly what the IRS has done. From 2005 to 2012, the agency seized more than $242 million for suspected structuring violations, in more than 2,500 cases. Institute for Justice, D. Carpenter & L. Salzman, *Seize First, Question Later: The IRS and Civil*

---

[4] *See* Bureau of Labor Statistics, U.S. Dep't of Labor, CPI Inflation Calculator, https://data.bls.gov/cgi-bin/cpicalc.pl (calculating that $10,000 in January 1970 was worth $64,802.91 in June 2017).

[5] *See, e.g.*, Compl. for Forfeiture (Doc. 1) ¶ 11, *United States v. $33,244.86 in U.S. Currency from TCF Nat'l Bank Account #XXXXXX6598*, No. 2:13-cv-13990-RHC-DRG (E.D. Mich. filed Sept. 18, 2013); Compl. for Forfeiture (Doc. 1) ¶ 12, *United States v. $35,651.11 in U.S. Currency Seized from PNC Account No. XXXXXX6937*, No. 4:13-cv-13118 (E.D. Mich. filed July 19, 2013); First Am. Compl. For Forfeiture *In Rem* (Doc. 15) ¶¶ 8-9, *United States v. $107,702.66 in U.S. Currency Seized from Lumbee Guaranty Bank Account No. XXXX2495*, No. 7:14-cv-00295-F (E.D.N.C. filed Apr. 30, 2015).

Forfeiture (Feb. 2015), at 10, http://ij.org/wp-content/uploads/2015/03/seize-first-question-later.pdf. The vast majority of those seizures – 86% – led to civil forfeiture actions, not criminal ones. *Id.* at 14. And, as the Treasury Inspector General recently determined, "structuring seizures primarily involved legal source funds from businesses." Treasury Inspector General for Tax Administration, *Criminal Investigation Enforced Structuring Laws Primarily Against Legal Source Funds and Compromised the Rights of Some Individuals and Businesses*, Ref. No. 2013-30-025 (Mar. 30, 2017), at 9, www.treasury.gov/tigta/auditreports/2017reports/201730025fr.pdf.

Indeed, in 91% of structuring seizures reviewed by the Inspector General, there was *no evidence* that the structured funds came from an illegal source or involved any other illegal activity. *Id.* Accordingly, the IRS's forfeiture program "was not conducted in a manner consistent with its stated goal of interdicting criminal enterprises." *Id.* at 8. Instead, IRS agents acted on instructions from United States Attorney's offices to make "quick hits" of people's bank accounts based on secret reviews of their banking behavior. *Id.* at 9-10. Based on these secret reviews, the United States Attorney would then seek a seizure warrant for the money in the account. *Id.* at 9, 13-16. In 92% of such cases, the IRS interviewed property owners only *after* their accounts were seized. *Id.* at 15. And in 97% of cases, property owners were not advised of their rights prior to these interviews. *Id.* at 19. These practices ensured that "judges did not possess information from

interviews with the property owner when making their probable cause determination," which, the Inspector General observed, "could have provided the judge with a possible explanation for the banking transactions to consider before signing the seizure warrant." *Id.* at 16.

Therefore, the cases of Carole, Randy, and Karen are illustrations of a broader national effort to seize property from legitimate businesses based on the sweeping surveillance power of *Miller*. Thousands of other property owners have faced the same Orwellian nightmare.

1. The Internal Revenue Service used the categorical approach to the Third Party Doctrine to monitor Carole Hinders' bank account and wrongfully seize more than $32,000.

Carole Hinders opened Mrs. Lady's Mexican Food in Arnold's Park, Iowa, in 1977. Mrs. Lady's was a family restaurant run by Carole, her mother, and her son, Josh. Because the business accepted only cash and checks, Carole made frequent deposits at a nearby bank. She developed a habit of depositing less than $10,000 at a time because her mother explained that deposits over that amount required extra paperwork and hassle at the bank. Carole understood this to mean that she would be stuck filling out pointless forms every time she deposited money, so she followed her mother's advice.

While Carole intended to avoid red tape at the bank, she had no desire to evade federal bank reporting laws. She believed that the "paperwork" she was avoiding was internal bank paperwork. She had no idea that this paperwork might be required by federal law – or that avoiding this paperwork could possibly be a federal crime.

Carole's forfeiture nightmare began in 2013, when the IRS seized all the funds in Mrs. Lady's bank account – $32,820.56. Carole had no prior warning. Nobody from the government or her bank asked why Carole was depositing money in amounts under $10,000. Nobody warned her that this depositing behavior could expose her to criminal liability for "structuring" her deposits.

Had anyone bothered to ask, they would have learned that Carole had nothing to hide. Indeed, the government acknowledged that Carole obtained the seized money legally. There was never any allegation that she had used the money for an illegal purpose or neglected to pay taxes or other financial obligations. The *only* suggestion of wrongdoing that the government ever made against Carole was that she "structured" the lawfully earned receipts of her legitimate restaurant business when she deposited the money in the bank.

Instead, the government seized Carole's money first and asked questions later. After monitoring her bank account without judicial oversight, the government obtained a warrant to seize the account based on

the affidavit of an Iowa police officer acting under the aegis of an IRS task force. His investigation prior to the seizure consisted solely of reviewing Carole's history of bank deposits, a history available to him only due to the Third Party Doctrine. He identified 55 cash deposits into Mrs. Lady's account between April 2012 and February 2013. Of these deposits, just 37 were in amounts between $5,000 and $9,500; 15 were between $3,000 and $4,950; and 3 were between $1,000 to $2,200. Verified Compl. of Forfeiture In Rem (Doc. 1), Ex. 2: Affidavit of Christopher Adkins ¶ 13, *United States v. $32,820.56 in U.S. Currency*, No. C13-4102-LTS (N.D. Iowa filed Oct. 24, 2013). From these 55 deposits, the agent selected 22 made on consecutive banking days that, when combined, totaled more than $10,000. *Id.* ¶ 14. Based on this pattern of deposits alone, he drew the following conclusion: "[T]he person doing the transactions, herself or someone on her behalf, structured the cash transactions in Mrs. Lady's [bank account] to avoid the preparation and submission of [currency transaction reports]." *Id.* ¶ 15. Had the IRS agent asked Carole before seizing her bank account, he would have known that she had no desire to avoid currency transaction reports – a key element of the crime underlying the seizure of her account. *See United States v. Sweeney*, 611 F.3d 459, 469-70 (8th Cir. 2010); *accord United States v. Van Allen*, 524 F.3d 814, 820 (7th Cir. 2008); *MacPherson*, 424 F.3d at 189.

In the months following the seizure, Carole met with the government's attorneys and attempted to persuade them of their mistake. She explained the

innocent reasons for her depositing behavior and voluntarily produced business and accounting records showing that she had nothing to hide. These efforts proved fruitless, however, when the government filed a civil forfeiture complaint to take Carole's money.

The government's forfeiture complaint was, if anything, even more perfunctory than the affidavit supporting the seizure of her account. No effort was made to explain why Carole would have wanted to avoid federal bank reporting requirements; the government did not allege (for instance) that Carole was attempting to evade taxes or launder the proceeds of a criminal enterprise. *See* Verified Compl. of Forfeiture In Rem (Doc. 1), *United States v. $32,820.56 in U.S. Currency*, No. C13-4102-LTS (N.D. Iowa filed Oct. 24, 2013). From the beginning of the case, therefore, there was no dispute that Carole's money all came from a legal source – her legitimate restaurant.

Carole's misfortune became a topic of national debate when the *New York Times* reported on her case and those of two other small business owners ensnared in similar proceedings.[6] Many other media outlets – both local and national – picked up the story.[7] For

---

[6] *See* Shaila Dewan, *Law Lets I.R.S. Seize Accounts on Suspicion, No Crime Required*, N.Y. Times, Oct. 26, 2014, at A1, http://www.nytimes.com/2014/10/26/us/law-lets-irs-seize-accounts-on-suspicion-no-crime-required.html.

[7] *See, e.g.*, *When the Government Charges Your Property With a Crime, Not You*, Iowa Public Radio, Nov. 5, 2014, iowapublicradio.org/post/when-government-charges-your-property-crime-not-you#stream/0 (45-minute interview with Carole and others); *Thieves in Suits*, Richmond Times-Dispatch, Oct. 29, 2014, www.richmond.

example, the *Des Moines Register* covered the case extensively and editorialized in favor of federal reforms in light of Carole's case.[8]

The IRS responded to these stories with official assurances that it would end its practice of seizing lawfully earned, lawfully spent money as it had done in Carole's case. This new IRS policy, first announced in the pages of the *New York Times*, prohibits agents from seizing money from a "legal source" (like a restaurant) based on "structuring" violations unconnected to another crime.[9]

---

com/opinion/our-opinion/editorial-thieves-in-suits/article_aaac41c4-8e8c-5db5-9a8f-c1e67790b7fd.html (editorial calling for federal forfeiture reform).

[8] *Congress must end abuses of seizures by feds*, Des Moines Register, Nov. 8, 2014, www.desmoinesregister.com/story/opinion/editorials/2014/11/08/congress-must-stop-seizures/18728827/; Daniel P. Finney, *Forfeiture target calls it, 'a violation of civil rights'*, Des Moines Register, Nov. 2, 2014, www.desmoinesregister.com/story/news/crime-and-courts/2014/11/02/civil-forfeiture-iowa-carole-hinders-arnolds-park/18362299/.

[9] Under the new policy, depositing cash in amounts less than $10,000 "should be treated as just an indicator that another violation of law might have occurred [and that] [t]herefore, authorized investigative activities should be performed to determine the source of the funds and if there are other related violations of law that should be investigated prior to initiating a seizure of funds related to the criminal activities." *See* IRS, U.S. Dep't of Treasury, Memorandum for Special Agents in Charge: IRS Structuring Investigation Policy Changes (Oct. 17, 2014), *available at* http://ij.org/wp-content/uploads/2015/07/IJ068495.pdf; *Statement of Richard Weber, Chief of I.R.S. Criminal Investigation*, N.Y. Times, Oct. 25, 2014, www.nytimes.com/2014/10/26/us/statement-of-richard-weber-chief-of-irs-criminal-investigation.html.

The Department of Justice followed suit with similar policy changes a few months later.[10]

But the government did not immediately end its case against Carole. At the same time it was providing public assurances of reform, in court filings, the IRS continued to accuse Carole of wrongdoing. Government lawyers insisted on taking her deposition. When Carole told them the truth – that she never even knew about the bank reporting laws – they agreed to dismiss their case without prejudice. In an effort to avoid paying attorneys' fees, costs, and interest, however, the IRS reserved the right to refile the case.[11] *See United*

---

[10] The Attorney General's memorandum and policy directive are available on the DOJ's website, www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/31/ag-memo-structuring-policy-directive.pdf.

[11] When Carole moved for attorneys' fees, costs, and interest under the Civil Asset Forfeiture Act of 2000 (CAFRA), 28 U.S.C. § 2465(b)(1), the government revived its threat to refile. Carole's motion was denied because the District Court, and later the Eighth Circuit, held that she did not "substantially prevail" within the meaning of CAFRA when the government dismissed its case without prejudice. *United States v. $32,820.56 in U.S. Currency*, 838 F.3d 930, 932, 937 (8th Cir. 2016). Nevertheless, judges at both levels chided the government for mistreating Carole. *See id.* at 938 (Erickson, J., concurring) ("The tortuous history of this case reflects an unwise exercise of discretion early on in the proceedings. It should have been apparent to the government and its agents that if Hinders had simply made daily cash deposits, no forfeiture question would have been raised."); *United States v. $32,820.56 in U.S. Currency*, 106 F. Supp. 3d 990, 995 (N.D. Iowa 2015) ("I fully understand the Claimants' frustration with this situation. After seizing their money and causing them to incur substantial expenses over a long period of time to fight that seizure, the Government elected to drop the case, effectively saying 'never

States v. $32,820.56 in U.S. Currency, 79 F. Supp. 3d 927 (N.D. Iowa 2015). Finally, the IRS released its hold on the $32,820.56 and returned all of the money to Carole's bank account – just over 21 months after it was seized.

2. Randy and Karen Sowers received the same treatment and had more than $62,000 wrongfully seized.

Randy and Karen had a similar experience, although they waited twice as long for the return of their money.

Randy and Karen run South Mountain Creamery – a dairy farm in Frederick County, Maryland. Randy and Karen's business is in the same rural community where they were born, married, and have lived their entire lives. They purchased their first 100 cows together in 1981. Since then, they have worked virtually without pause to care for their animals and grow their business. More than 30 years after opening their farm, they still wake before dawn every day to milk their cows.

Because of the nature of their business, Randy and Karen often deposit cash in the bank. Customers at farmers' markets frequently pay in cash and the size of Randy and Karen's cash deposits varies depending on the number of farmers' markets that they visit and

---

mind.' The return of the seized funds hardly makes the Claimants whole.").

the amount of milk, eggs, and other products that they sell. Sometimes Randy and Karen have less than $10,000 in cash to deposit, but sometimes they have more.

Like Carole, Karen typically deposited cash in amounts under $10,000 because she was advised to do so. After one particularly busy weekend in 2011, a bank teller told Karen that cash deposits over $10,000 would require "paperwork." The teller suggested that this paperwork would be time-consuming for bank personnel to fill out and that Karen could make life easier for bank employees by keeping the size of her deposits under $10,000. Karen did not know what this paperwork involved. The teller said nothing about the IRS, and, for all Karen knew, the paperwork was required by internal bank rules with no connection whatsoever to the federal government. Karen generally kept some cash on hand to make change and to help cover expenses at the store and, given the teller's advice, it seemed reasonable to hold enough cash in reserve to keep the size of the deposits under $10,000. Karen did this to avoid red tape at the bank – not to hide information from the IRS.

Without any notice, in February 2012, the IRS seized the farm's entire bank account, containing $62,936.04. Apart from the act of depositing cash in amounts less than $10,000, the government never even *alleged* that Randy and Karen did anything illegal.

After taking Randy and Karen's money, the government presented them with an offer they could not

afford to refuse. They could go to court and fight for months or even years to contest the forfeiture – likely spending more in attorney fees than the amount that had been seized – or they could agree to forfeit $29,500 of the approximately $63,000 that was taken. Even though Randy and Karen believed they had done nothing wrong, they needed the seized money for their farming operations and could not afford a protracted legal battle to prove their innocence. So, like other property owners faced with this choice, Randy and Karen reluctantly agreed to forfeit $29,500 of their hard-earned money.

After the IRS and DOJ changed their structuring policies, Randy and Karen filed a petition with the government seeking the return of their $29,500. *See* Pet. for Remission or Mitigation (July 16, 2015), *available at* http://ij.org/wp-content/uploads/2015/07/irs-forfeiture-petitions-randy-sowers-petition.pdf. Their petition got a boost when Members of Congress condemned what had happened to them at a hearing where Randy was called to testify. *See id.*, Ex. C at 86 (statement of Rep. Crowley) ("Mr. Sowers . . . I don't think you, nor any of the gentlemen before us today, deserve to be treated by your Government, by the IRS, in the way in which you have been."). Representative John Lewis told Randy, "as one Member of Congress and a member of this committee, I want to apologize to you for . . . what the IRS did to you." *Id.*, Ex. C at 93.

In June 2016, the Department of Justice granted Randy and Karen's petition and returned their $29,500. The four-year span of this legal drama was

extremely difficult for Randy and Karen. Randy was forced to scramble to replace money that he had planned to use to buy supplies for that year's crops and ultimately had to divert money that he otherwise would have used to pay off debts or grow the business. Meanwhile, although Karen has always been careful to avoid bouncing checks, she found herself forced to explain to business partners why scheduled transactions were not going through. The bank where they had done business over a decade summarily closed their account. Randy and Karen worried that people would assume they must have committed a serious violation of the law to have had their money seized, and in fact they became aware that they were the subject of hurtful gossip in their community. Karen found the situation so stressful that she became ill. And Randy was left wondering how something like this could possibly happen in America.

II. This Court Should Reject the Categorical Approach to the Third Party Doctrine.

What happened to Randy, Karen, and Carole was possible only because there is no constitutional limitation on blanket surveillance of people's banking practices. Their experiences should give this Court pause before extending the categorical rule of *Miller* to the world of cell-site-location information (CSLI). As one member of this Court has pointed out, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is

ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (citations omitted). Such caution is warranted in the realm of CSLI because, even using present-day technology, CSLI can reveal far more about a person's private affairs than bank records ever could. As shown below, these considerations counsel against applying a pre-digital precedent like *Miller* to this digital-age case.

A. Applying the categorical approach of *Miller* to the cell-site-location information in this case would lead to the same dragnet surveillance of phone information that the nation has experienced in banking.

When this Court decided *Miller*, in 1976, computer technology was in its infancy. Computer usage was uncommon and most business records were kept on paper. Although data mining – the practice of using computer algorithms to search vast collections of data for patterns – is common practice in business and government today, it was barely a concept in the late 1970s. In other words, despite the sweeping surveillance power created by *Miller*, practical technological limitations ensured that the Third Party Doctrine, even if fully exploited by law enforcement, could have only a limited impact on privacy. But in the years since *Miller*, widespread advances in computer technology have given government the capacity to search broad

swaths of data looking for suspicious activity. This in turn has led to innocent people becoming ensnared in civil forfeiture proceedings, in which the government can profit from seizing property without charging a person with any crime.

This past is prologue; it demonstrates the threat that a categorical Third Party Doctrine poses to property rights and privacy in the digital age. As other *amici* have pointed out, cell phones are no longer a luxury; instead, more than 91% of American adults own a cell phone and most carry it with them everywhere they go. Brief for Electronic Frontier Foundation et al. as *Amici Curiae* in Support of Certiorari at 4. Everyone who uses a cell phone generates CSLI, just as everyone who uses a bank generates bank records. But CSLI reveals far more about a person than any conventional bank record could and does so on a scale unrivaled even by the staggering amount of bank reporting that occurs every day in this country. *See*, *supra*, pp. 11-13.

Each time a cell phone connects to a cell tower, it generates information about where the phone was located at that moment in time. This happens with surprising frequency: Cell phones connect with towers on average every seven to nine minutes – or between 160 and 205 times per day – although they can connect as frequently as every seven seconds. *See* Brief for Electronic Frontier Foundation et al. as *Amici Curiae* in Support of Certiorari at 9. As cell phone and data usage have both increased, the number of cell towers has increased, as well, leading to more precise location information about individual users. Using current

technology, cell companies can provide an accurate picture of a phone's location to within 50 meters. *Id.* at 11. As technology continues to improve, CSLI is likely to provide an ever-more detailed picture of a person's movements. *See In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 755 (S.D. Tex. 2005) (noting the "combination of market and regulatory stimuli ensures that cell phone tracing will become more precise with each passing year"). Past experience with technology suggests what today can be measured within 50 meters will, in just a few years, be measurable to within five.

This increasingly granular picture of a person's movements provides law enforcement with a powerful tool to fight crime, but it also raises chilling privacy concerns. Just as GPS tracking "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring), so too with CSLI. It seems likely that, within a few years, CSLI will be able to place a person within a particular room in their home. *See* Brief for Electronic Frontier Foundation et al. as *Amici Curiae* in Support of Certiorari at 15 (noting that the ACLU was able to use CSLI to "infer details about [a person's] patterns of movement, including when he and his pregnant wife visited her obstetrician, when he traveled to or from his home, and nights he spent away from home") (citation omitted). Even today, by comparing the CSLI of one person to that of another, law enforcement can diagram a

person's associations and lifestyle, including such intimate information as whether that person is expecting a child. *See id.*

The Stored Communications Act, 18 U.S.C. § 2703, offers inadequate privacy protections in such situations. *See* Brief for Petitioner at 47-53. Nothing in the Act prohibits the bulk collection of cell phone records when the government shows "specific and articulable facts" that the records are "relevant and material to an ongoing criminal investigation." *See* 18 U.S.C. § 2703(b), (d). In practice, this is a low bar. In this case, law enforcement obtained five-months' worth of CSLI for six different suspects. *See* Pet. App. 49a-61a. At least nine other phone numbers were swept up in the investigation, as reflected in the District Court's record. *See* United States' Combined Br. & Resp. to Defs.' Mots. in Limine, Ex. 2, at 2-3, *United States v. Carpenter*, No. 2:12-cr-20218-SFC-MKM-4 (E.D. Mich. filed Dec. 24, 2013), ECF No. 221-2. Indeed, prosecutors in this case successfully argued that "relevant and material" is a low standard. *See* Brief for Petitioner at 48 (quoting J.A. 34) ("We merely have to show there's a criminal investigation of a crime."). Moreover, what matters here is not the statutory minimum set by Congress, but the constitutional minimum set by this Court.

If CSLI is categorically exempt from Fourth Amendment protection, it is reasonable to presume that the government would obtain CSLI to track people over the course of weeks, months, or even years. Computer algorithms could then mine that data,

looking for instances when people went to the "wrong" neighborhood, business, or home, or when they associated with the "wrong" individuals. The government could build a portrait of a person's friends, family, and associates. And, when a crime is committed, everyone in the vicinity could be easily located and their movements reconstructed.

Police and prosecutors could use this information for criminal prosecutions or they could use it to pursue civil forfeiture without charging a crime. Past experience suggests that they would often choose civil forfeiture. Department of Justice statistics show that, between 1997 and 2013, 87% of forfeitures were pursued in civil, not criminal cases. Institute for Justice, *Policing for Profit*, at 12-13. This means that the owner of seized property is almost *seven times* more likely to face a civil forfeiture proceeding than a criminal proceeding. In a civil proceeding, the property owner will have no right to an attorney, the government's burden is a mere preponderance of the evidence, and an innocent third-party will bear the burden of proving her innocence. By comparison, in a criminal proceeding, there *is* a right to an attorney and the burden is squarely on the government to prove its case beyond a reasonable doubt. No wonder that government strongly prefers civil cases. This already bad situation for property owners would only be made worse if the government enjoys warrantless access to CSLI.

For example, imagine a case involving a roadside seizure of cash. Police find a man traveling with $5,000 in his car. He claims the money constitutes his

personal savings, but police are suspicious he is transporting drug proceeds. No drugs are found, but police are able to use CSLI to place the man at the residence of a convicted drug dealer hours before he was pulled over. In the world of civil forfeiture, where the government's only burden is to show a preponderance of the evidence, this would likely be enough to forfeit the man's money (and possibly his car), even though it would never be sufficient to convict him of a crime. *See, e.g.*, *United States v. Funds in the Amount of $30,670*, 403 F.3d 448, 469 (7th Cir. 2005) (combination of dog sniff and circumstantial evidence sufficient to establish forfeitability of seized currency at summary judgment); *United States v. $174,206.00 in U.S. Currency*, 320 F.3d 658, 662 (6th Cir. 2003) (affirming summary judgment for the government based on property owners' lack of legitimate income and absence of rebuttal showing a legitimate source). Even if the officers' suspicions turned out to be wrong because the man could affirmatively demonstrate a legitimate source for his funds, nothing would stop them from seizing his money on the side of the road. Seizure, with no judicial oversight, could be based on a warrantless review of CSLI, thereby placing the burden on the property owner to get a lawyer and fight the seizure in court – a fight that, as shown above, can take property owners months, if not years, to win.

Interposing a warrant requirement in these circumstances would make wrongful seizures less likely. Certainly, a warrant requirement is not cost free. Warrants require time and effort on the part of officers,

prosecutors, and courts. But the absence of a warrant requirement also has a cost. Warrantless searches of CSLI will inevitably lead to wrongful seizures, which will force property owners to expend weeks, months, even years working to recover their lawful money. Indeed, as illustrated by the experiences of Carole, Randy, and Karen, there is a human cost when the government accuses an innocent person of wrongdoing, a cost that remains even when the innocent are ultimately vindicated.

Through this lens, this Court should consider the consequences of holding that CSLI is categorically unprotected by the Fourth Amendment. This case concerns one man's crime spree, but the rule announced here will affect innocent people as much (if not more) than criminals. If the Court gives the government unfettered access to CSLI, innocent people's movements, habits, and associations will become known to the government. Past experience suggests that many of these innocent people will be drawn into civil forfeiture proceedings. Sometimes the government will get it right; other times it will wrongly seize property, just as it did in Carole, Randy, and Karen's cases. Rejecting the categorical approach of *Miller* would at least impose a measure of judicial scrutiny in an area of the law which sorely needs it.

B. The Court should reject the categorical approach to the Third Party Doctrine and instead adopt a real-world approach that scrutinizes positive law, including statutes and private contracts.

The categorical approach to the Third Party Doctrine, as articulated by cases like *Miller* and *Smith*, has proven itself to be a failure. By holding that a person loses all constitutional protection in any information that person has entrusted to another private party, even when those parties explicitly agreed to keep such information private, *Miller* and *Smith* have enabled the very kind of dragnet surveillance that the Fourth Amendment is meant to stand guard against. This infirmity, coupled with the powerful financial incentive underlying civil forfeiture, has had disastrous effects on ordinary Americans like Carole Hinders and Randy and Karen Sowers. A decision extending the categorical approach to the Third Party Doctrine into the world of CSLI would unleash a parade of horribles even worse than the experiences of *amici* described above.

Thankfully, this Court can choose a wiser path. Rather than asking whether a person who shares information retains a reasonable expectation of privacy in that information, this Court should refine its approach to ask a more pertinent question: Is the government demanding access to information that would otherwise be unavailable to private parties? This has been called the "positive law" approach to the Third

Party Doctrine because it would evaluate the government's power to search a person and seize their things based on what the law allows private individuals to do. *See* William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv. L. Rev. 1821, 1871-77 (2016). The virtue of the positive law model is that it embodies a simple yet powerful intuition: That when government officials use their power to obtain information in a manner that would be prohibited for private actors, those officials must demonstrate the reasonableness of their actions under the Fourth Amendment. Thus, by requiring that a neutral magistrate determine that there is probable cause for an investigation, the positive law model helps ensure the unique powers of government actors are checked by an independent judiciary.

The positive law model proposed by Professors Baude and Stern is far more protective of an individual's privately shared information than the current Third Party Doctrine. This is because, rather than holding that such information is categorically unprotected, the new model would ask if the government's efforts rest on conduct to which officials hold some special privilege. And that answer, in turn, would rest not on abstract notions of "reasonable expectations of privacy," but instead on the concrete statutory and contractual arrangements that form the positive legal background.

This approach offers a fresh perspective on this case. Under the positive law model, the government

would be required to meet Fourth Amendment reasonableness standards before obtaining CSLI because cell phone companies are legally prohibited from disclosing their customers' location information to other private parties "without the express prior authorization of the customer." 47 U.S.C. § 222(f). Under reasonableness analysis, government attempts to coerce or compel the disclosure of such information would almost certainly require a warrant – and therefore a finding of probable cause by a neutral magistrate – for the simple reason that background principles of property and contract law rarely if ever empower private individuals to compel a third party to disclose information.

Implementing this model does not require a wholesale revision of Fourth Amendment jurisprudence. *See* Richard M. Re, *The Positive Law Floor: Responding to William Baude & James Y. Stern, The Positive Law Model of the Fourth Amendment*, 129 Harv. L. Rev. F. 313 (2016). It only requires that the government justify its actions under the Fourth Amendment when it has intruded on someone's privacy in a manner that a private party could not. This approach would resolve the problems caused by the categorical Third Party Doctrine, provide firmer guidance to lower courts, and retain the ability of courts to find that a "reasonable expectation of privacy" has been violated even in instances where the positive law model is not triggered.

A degree of individualized judicial scrutiny is also nothing to fear. Requiring that the government meet

Fourth Amendment reasonableness standards would both ensure that the government's actions are reasonable in each particular instance and, more broadly, would protect against the government's assembly of a digital dragnet that could enable widespread location monitoring. And, perhaps most importantly, it would help to guard against the kind of forfeiture horror stories experienced by *amici* and countless others.

CONCLUSION

Forty-one years ago, in *United States v. Miller*, this Court announced a categorical rule that applied the Third Party Doctrine to allow the warrantless search and seizure of Americans' banking information. The decision in *Miller* has had disastrous effects in banking. If that same categorical approach were applied to CSLI, it could make vastly more sensitive information available to the government without a warrant. The Fourth Amendment's warrant requirement should not be read out of the Constitution in this way. Police and prosecutors should be required to show probable cause to a neutral magistrate before they can scrutinize the digital information that, in this day and age,

we are all passively creating about ourselves every hour of every day.

Respectfully submitted,

INSTITUTE FOR JUSTICE
WESLEY HOTTOT*
10500 Northeast 8th Street,
Suite 1760
Bellevue, WA 98004
Tel: (425) 646-9300
E-mail: whottot@ij.org

ROBERT P. FROMMER
901 North Glebe Road, Suite 900
Arlington, VA 22203
Tel: (703) 682-9320
E-mail: rfrommer@ij.org

**Counsel of Record*

Counsel for Amici Curiae

RECORD AND BRIEFS

No. 16-402

Supreme Court, U.S.
FILED
SEP 2 - 2017
OFFICE OF THE CLERK

In The

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ Of Certiorari To The United States Court Of Appeals For The Sixth Circuit

BRIEF OF PROFESSOR ORIN S. KERR AS AMICUS CURIAE IN SUPPORT OF RESPONDENT

ORIN S. KERR
Counsel of Record
2000 H Street, NW
Washington, DC 20052
(202) 994-4775
okerr@law.gwu.edu

TABLE OF CONTENTS

Page

TABLE OF CONTENTS i

TABLE OF AUTHORITIES iii

INTEREST OF THE AMICUS CURIAE 1

SUMMARY OF ARGUMENT 1

ARGUMENT 2

I. COLLECTION OF HISTORICAL CELL-SITE DATA IS UNPROTECTED BY THE FOURTH AMENDMENT BECAUSE IT IS THE NETWORK EQUIVALENT OF OBSERVATION IN PUBLIC SPACE 3

II. THE BALANCE OF PRIVACY AND SECURITY IN HISTORICAL CELL-SITE RECORDS IS BEST RESOLVED BY LEGISLATION SUCH AS THE STORED COMMUNICATIONS ACT 7

(a) Cell Phones Can Be Used to Facilitate Crime 9

(b) Encryption Limits Government Communications Surveillance Power 11

(c) Congress and State Legislatures are Actively Engaged in Deciding the Proper Statutory Protection For Cell-Site Records 12

III. THE COURT SHOULD REJECT CARPENTER'S MOSAIC THEORY OF THE FOURTH AMENDMENT 15

TABLE OF CONTENTS – Continued

Page

IV. WHETHER REASONABLE PEOPLE EXPECT PRIVACY IN CELL-SITE RECORDS IS IRRELEVANT, AS THE THIRD PARTY DOCTRINE IS ABOUT MANIFESTING SUBJECTIVE EXPECTATIONS OF PRIVACY 20

V. THE ENACTMENT OF PRIVACY LEGISLATION DOES NOT GOVERN OR INFLUENCE THE MEANING OF THE FOURTH AMENDMENT 26

(a) Privacy Legislation Does Not Provide Evidence of Reasonable Expectations of Privacy 26

(b) 47 U.S.C. § 222 Does Not Make Cell-Site Records the User's Fourth Amendment "Papers" 29

CONCLUSION 30

TABLE OF AUTHORITIES

Page

CASES

Berger v. New York, 388 U.S. 41 (1967) 11

Dunaway v. New York, 442 U.S. 200 (1979) 15

Ex Parte Jackson, 96 U.S. 727 (1878) 7

Hester v. United States, 265 U.S. 57 (1924) 21

Hoffa v. United States, 385 U.S. 293 (1966) 21, 22, 23

Johnson v. United States, 333 U.S. 10 (1948) 10

Katz v. United States, 389 U.S. 247 (1967) ..... *passim*

Lewis v. United States, 385 U.S. 206 (1966) 21

Lopez v. United States, 373 U.S. 427 (1963) 22

Minnesota v. Carter, 525 U.S. 83 (1998) 29

New York v. Belton, 453 U.S. 454 (1981) 15, 19

On Lee v. United States, 343 U.S. 747 (1952) 22

Osborn v United States, 385 U.S. 323 (1966) 22

Riley v. California, 134 S. Ct. 2473 (2014) 8, 13, 15, 20

Rios v. United States, 364 U.S. 253 (1960) 21

Smith v. Maryland, 442 U.S. 735 (1979) 7

State v. Gray, 234 N.C. App. 197 (2014) 10

Terry v. Ohio, 392 U.S. 1 (1968) 9

United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016) 29

United States v. Dionisio, 410 U.S. 1 (1973) 3

TABLE OF AUTHORITIES – Continued

Page

United States v. First National Bank, 295 F. 142 (S.D. Ala. 1924), *aff'd*, 267 U.S. 576 (1925).....7

United States v. Hill, 2013 WL 11317131 (N.D. Okla. 2013).....10

United States v. Horton, 863 F.3d 1041 (8th Cir. 2017).....8

United States v. Jacobsen, 466 U.S. 109 (1984).....25

United States v. Jeffers, 342 U.S. 48 (1951).....21

United States v. Jones, 565 U.S. 400 (2012).....15, 16

United States v. Olusola, 564 Fed.Appx. 466 (11th Cir. 2014).....10

United States v. Supreme Court of N.M., 839 F.3d 888 (10th Cir. 2016).....28

CONSTITUTIONAL PROVISIONS

Supremacy Clause.....28

U.S. Const. Amend. IV .....*passim*

STATUTES

18 U.S.C. § 2702 .....12, 24

18 U.S.C. § 2703 24

18 U.S.C. § 2703(d).....12, 20

47 U.S.C. § 222 .....26, 29

TABLE OF AUTHORITIES – Continued

Page

Cal. Penal Code
§ 1546(d) 14
§ 1546.1(b)(1) 14
§ 1546.1(d) 14

Pub. L. No. 103-414, Title II, § 207(a) (1994) 13

OTHER AUTHORITIES

Berin Szóka, *Privacy Reform Finally Moves in House: Goodlatte Promises Geolocation Privacy Bill Will Move Soon*, Tech Policy Corner, Apr. 14, 2016 14

EFF Statement on and Analysis of Digital Telephony Act, October 8, 1994 13

Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 Stan. L. Rev. 1049 (2000) 30

Jake Swearingen, *No, the CIA Hasn't Compromised Signal and WhatsApp*, N.Y. Mag. Select All, Mar. 7, 2017 11

Orin S. Kerr, *A User's Guide to the Stored Communications Act, And A Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208 (2004) 12

Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311 (2012) 15, 17

TABLE OF AUTHORITIES – Continued

Page

Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, Geo. L.J. (forthcoming 2018), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033 12

Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev. 476 (2011) 7, 8, 11

Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005 (2010) 4, 5, 6

Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan. L. Rev. 503 (2007) 20

Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. Chi. L. Rev. 113 (2015) 21, 23, 24

Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, 115 Mich. L. Rev. 1117 (2017) 27, 28, 29

Patricia M. Wald, *Some Observations on the Use of Legislative History in the 1981 Supreme Court Term*, 68 Iowa L. Rev. 195 (1983) 28

Susan Freiwald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA)*, Berkeley Tech. L.J. (forthcoming 2018) 14

INTEREST OF THE AMICUS CURIAE

Orin S. Kerr is the Fred C. Stevenson Research Professor at the George Washington University Law School. Beginning in January 2018, he will be a Professor of Law at the University of Southern California Gould School of Law. The interest of amicus is the sound development of Fourth Amendment law.[1]

SUMMARY OF ARGUMENT

The Fourth Amendment does not apply to the collection of historical cell-site records. Collection of historical cell-site records is the network equivalent of unprotected observation in public space. Because the effect of technological change is uncertain and evolving, the Court should allow Congress and state legislatures to continue their active and dynamic debates about the proper regulation of historical cell-site records. The Court should also reject Carpenter's mosaic theory of the Fourth Amendment. The third-party doctrine should be retained, but the Court should restore it to its proper place as the subjective expectation of privacy test.

[1] All parties have consented in writing to the filing of this brief. No entity or person aside from amicus curiae made any monetary contribution supporting the preparation or submission of this brief. No counsel for any party to this proceeding authored this brief in whole or in part.

ARGUMENT

This is a challenging case. The facts involve new and developing technology. The law features vague and often-criticized tests. And the Court can't help but feel pulled by two competing and legitimate concerns. On one hand, the law must keep up as technology changes to maintain privacy protections. On the other hand, the blunt instrument of the Fourth Amendment shouldn't be forced beyond its proper role.

This brief offers a way through the difficult issues in five steps. It begins by anchoring the legal issues raised in the familiar context of the physical world. It then considers whether technological change justifies a departure from the Court's traditional rules. After that, it explains why the Court should reject the theory Carpenter advocates that would draw a distinction between longer-term and shorter-term surveillance. It next explains how the parties have misunderstood a significant part of the case, and how the case becomes much simpler when properly understood. The brief concludes by discussing the proper relationship between the interpretation of the Fourth Amendment and statutory law.

I. COLLECTION OF HISTORICAL CELL-SITE DATA IS UNPROTECTED BY THE FOURTH AMENDMENT BECAUSE IT IS THE NETWORK EQUIVALENT OF OBSERVATION IN PUBLIC SPACE.

Obtaining historical cell-site records from a cell phone provider is like obtaining testimony from an eyewitness to suspicious conduct. By contracting with a cell phone network provider to deliver their calls, customers ensure that network providers may be available to testify – whether in person or by sending records – about how the providers made that delivery for their users. Just as a person voluntarily exposes himself to observation by traveling in public to deliver a communication, so does a person voluntarily expose himself to observation by hiring an agent to deliver his communications remotely. The Fourth Amendment is not implicated by compelling testimony from an eyewitness or by observation in public. *See United States v. Dionisio*, 410 U.S. 1, 8-10 (1973); *Katz v. United States*, 389 U.S. 247, 361 (1967) (Harlan, J., concurring). The same rule should apply in the analogous context of obtaining historical cell-site records.

To appreciate this perspective, it is essential to realize that the Fourth Amendment traditionally achieves a balance between protected and unprotected conduct. On one hand, the Fourth Amendment extends constitutional protection to a person's "houses, papers, and effects" from unwarranted government interference. U.S. Const. Amend. IV. On the other hand, the

Fourth Amendment offers no protection from government surveillance in public. *See Katz*, 389 U.S. at 361.

A useful approximation of the Court's many cases is that the Fourth Amendment protects what occurs inside but doesn't protect what occurs outside. *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1009-11 (2010) (hereinafter *General Approach*). This dividing line strikes an essential balance in physical-world investigations. It limits government power to protect privacy in some spaces (inside), but it allows the government to investigate without restriction in other spaces (outside). *See id.* at 1011.

When applying the Fourth Amendment to communications networks, the Court's first instinct should be to preserve this essential traditional balance. To ensure that the balance of the Fourth Amendment is maintained in our increasingly networked technological world, the Court should translate the law's treatment of physical world space across the shift to a networked environment. This is necessary to maintain the traditional degree of privacy protection the Fourth Amendment offers as technology changes.

Translation produces a simple rule: Although the Fourth Amendment protects the contents of communications sent over a network, it does not protect non-content addressing information used to deliver those contents. *See General Approach* at 1017-22. Judge Kethledge properly recognized in his opinion below that the Court's precedents have adopted the content/

non-content distinction in its caselaw on postal letters and telephone calls. Pet. App. 9a-13a. But the content/non-content line is essential for a deeper reason beyond precedent. It recreates the inside/outside distinction from the physical world, protecting the network equivalent of inside surveillance (contents) and leaving unprotected the network equivalent of outside surveillance (non-content records). *See General Approach* at 1017-22.

To see this, imagine a world without communications networks. If Alice wants to communicate with Bob, Alice has to leave her home and travel to Bob's house. If the police suspect that Alice and Bob are conspirators planning a crime, and they assign an officer to watch Alice's whereabouts, the police can collect only some information without triggering the Fourth Amendment. The police cannot learn the contents of what Alice and Bob said inside Bob's home without a warrant. On the other hand, the police can observe Alice and see what she did in public – when she left home, where she traveled, when she arrived at Bob's house, and where they both live – without triggering the Fourth Amendment.

Next imagine that Alice calls Bob on her cell phone instead of meeting him in person. Alice no longer has to travel to meet Bob. The cell phone network delivers the call from Alice to Bob, making a remote transfer that eliminates the need for a public trip. But, critically, the same information exists. What was previously the contents of the conversation in Bob's house is now the contents of the phone call between Alice and

Bob. And what was previously Alice's publicly observable trip from her house to Bob's house is now a record that the phone provider generated and may keep about when the call was made, to and from what numbers, and what cell towers were used to deliver it.

To maintain the balance of the Fourth Amendment, courts should treat the same information in the same way in both the physical and network contexts. The contents of phone calls should be protected, as they are the telephone equivalent of protected inside space. This means, in the Internet context, that the contents of e-mails, text messages, and files that users place in cloud storage should receive full Fourth Amendment protection. *See General Approach* at 1029. On the other hand, non-content records generated by network providers – the business records they generate about how they delivered the communications – should not be protected because they are the network equivalent of the publicly observable trip that is outside such protection in the physical world. *See id.* at 1017-22.

It is true, as Carpenter argues, that cell phones are "indispensable for full participation in family, social, professional, civic, and political life." Petr. Br. at 40. But that provides no more reason to protect cell-site records than does the normal human need to venture outside provide reason to protect observation in public. The Fourth Amendment extends protection to some aspects of life but leaves other parts unprotected both in the physical world and in the network environment.

This approach should lead the Court to reaffirm the traditional rule, over a century old, that collection of non-content addressing information for a network communication does not implicate the customer's Fourth Amendment rights. *See Ex Parte Jackson*, 96 U.S. 727, 733 (1878) (postal letters); *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) (telephone calls). *See also United States v. First National Bank*, 295 F. 142, 143 (S.D. Ala. 1924) (rejecting a challenge to government access to a couple's entire bank records, stating that "[t]his is not a question of a search and seizure of a party's books and papers, but of whether a witness who has information as to a party's dealings may be required to testify to those facts"), *aff'd*, 267 U.S. 576 (1925) (per curiam).

II. THE BALANCE OF PRIVACY AND SECURITY IN HISTORICAL CELL-SITE RECORDS IS BEST RESOLVED BY LEGISLATION SUCH AS THE STORED COMMUNICATIONS ACT.

But wait, Carpenter says: Cell phone technology has expanded government power to invade privacy. In petitioner's view, changing technology justifies adding new protection for cell-site records to restore the prior level of government power. Petr. Br. at 14-21. I have called this argument "equilibrium-adjustment." I agree with Carpenter that, in a proper case, equilibrium-adjustment is an appropriate way to update Fourth Amendment rules in light of technological change. *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev. 476,

525-42 (2011) (hereinafter *Equilibrium-Adjustment*). Technological change that dramatically expands government power under old legal rules can justify imposing greater privacy protection. *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473, 2494 (2014) (requiring a warrant to search a cell phone incident to arrest because of "all they contain and all they may reveal"); *Equilibrium-Adjustment* at 525-42.

This is not such a case, however. First, Carpenter exaggerates the threat to privacy posed by historical cell-site records. Such records ordinarily cover too broad an area to be particularly revealing on their own. Resp. Br. at 24-28. Notably, Carpenter does not say what personal or sensitive fact was learned about him, other than his location generally near a string of robberies, when the government collected his records.[2] Carpenter's brief instead focuses on the privacy threat raised by different location technologies such as GPS

---

[2] The Technology Experts claim that the records show Carpenter "attended a particular church in Detroit nearly every Sunday." Brief of Amici Curiae Technology Experts at 29 n.49. That is wrong. According to an amicus brief filed in the Sixth Circuit, Carpenter told amicus counsel that he attended a particular church. *See* Brief of Amicus Curiae Am. Civil Liberties Union et al. at 11, 819 F.3d 880 (2016) (Nos. 14-1572 & 14-1805), available at https://www.aclu.org/legal-document/united-states-v-carpenter-amicus-brief. Analysis of the cell-site records then showed that on "a number of Sundays," Carpenter's phone was used in sectors that included that church. *Id.* This provides no basis to conclude that the records, considered alone, would have revealed church attendance. The reason to think Carpenter attended a particular church is that he said so.

tracking. *See* Petr. Br. at 19-29, 42-47. Those technologies typically require access to information stored inside a person's physical device, however, and therefore their use may be searches under traditional Fourth Amendment principles. *See, e.g.*, *United States v. Horton*, 863 F.3d 1041, 1047 (8th Cir. 2017).

More fundamentally, technology's impact on government communications surveillance power is decidedly mixed. Although cell phone technology expands government power in some ways, it shrinks government power in other ways that Carpenter ignores. A close look at two dynamics – how cell phones can facilitate crime and the role of encryption – suggests that the overall impact of technology on government surveillance power is uncertain and still evolving.

(a) Cell Phones Can Be Used to Facilitate Crime.

Cell phone technology can limit government power by giving wrongdoers a powerful new way to avoid detection in the commission of crime. Consider the impact of cell phones on a group robbery such as the one in this case. Before the cell phone age, conspirators planning to rob a store had to "case the joint" in the open and meet in person to coordinate their plans. Their suspicious behavior risked drawing the attention of officers nearby. *See Terry v. Ohio*, 392 U.S. 1 (1968) (permitting an officer to "stop and frisk" conspirators acting suspiciously in front of a store in the course of planning a robbery).

Cell phones make such crimes easier to commit and harder to detect. These days, robbery conspirators can coordinate their crimes silently and instantly over any distance by cell phone text message. One conspirator can watch the store and text his observations to the others. *See, e.g.*, *State v. Gray*, 234 N.C. App. 197, 206 (2014). A second conspirator can serve as a lookout and text the group if danger appears. *See United States v. Olusola*, 564 Fed.Appx. 466, 468 (11th Cir. 2014). After the robbery, the leader can text the rest with instructions about where to meet to divvy up the loot. *See, e.g.*, *United States v. Hill*, 2013 WL 11317131, *2 (N.D. Okla. 2013). The cell phone replaces awkward and suspicious in-person meetings with concealed, silent, and instant coordination. An officer walking the beat will be none the wiser. The conspirators will look like everyone else: Just people checking their phones.

The ways that cell phones can facilitate crime and avoid detection counsels against creating new Fourth Amendment protections for cell phone records. Obviously, most people don't use their phones to commit crimes. But most people don't have their records collected by court order under the Stored Communications Act, either. The key point is that the effect of cell phone technology on the "often competitive enterprise of ferreting out crime," *Johnson v. United States*, 333 U.S. 10, 14 (1948), operates as a two-way street. The ability of cell phone companies to deliver communications quickly and silently over any distance cuts both ways. It can lead to records about the delivery that helps the police, and it can aid in the commission of

crime that helps wrongdoers. Both should be considered. *See Equilibrium-Adjustment* at 512-17.

(b) Encryption Limits Government Communications Surveillance Power.

The rise of encryption also complicates the dynamic Carpenter describes. In the past, the government ordinarily had the technical capacity to intercept the contents of phone calls and communications. *See Berger v. New York*, 388 U.S. 41, 46 (1967). In the last decade, however, software providers have provided powerful and free technologies that enable anyone to shield the contents of their communications from lawful government access by encrypting the contents of their network communications during transmission. For example, today over one billion people worldwide use "WhatsApp," a program first introduced in 2009 that encrypts messages end-to-end. *See* Join WhatsApp.[3] As far as the public knows, not even the Central Intelligence Agency can break WhatsApp's encryption. *See* Jake Swearingen, *No, the CIA Hasn't Compromised Signal and WhatsApp*, N.Y. Mag. Select All, Mar. 7, 2017.[4] Doing so is presumably beyond the capacity of federal, state, or local law enforcement.

Encryption shows how the impact of technology on government communications surveillance power can work both ways. Encryption brings many wonderful

---

[3] https://www.whatsapp.com/join/

[4] http://nymag.com/selectall/2017/03/no-the-cia-hasnt-cracked-encrypted-chat-app-signal.html

benefits, but it can leave investigators unable to read a target's encrypted communications even with a search warrant. It is too early to tell how far encryption will interfere with government investigative powers.[5] But because users generally can't encrypt non-content records such as historical cell-site records, the collection of such records may take on a more important role in future surveillance practices. The Court should be reluctant to introduce new constitutional protections for non-content records when the existing constitutional framework for access to contents may be impeded by new encryption technology.

(c) Congress and State Legislatures are Actively Engaged in Deciding the Proper Statutory Protection For Cell-Site Records.

Because the effect of technology on communications surveillance is a mixed bag, the Court should continue to allow legislatures to debate and decide how much protection cell-site records should receive. The federal Stored Communications Act sets a floor for all investigators. *See* 18 U.S.C. § 2702, § 2703(d). *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, And A Legislator's Guide to*

---

[5] Law enforcement can try several ways to work around encryption to access contents. *See generally* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, Geo. L.J. (forthcoming 2018), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033. These methods may or may not work, however, and some require considerable resources beyond the reach of many criminal investigations. *See id.* at 33-35.

Amending It, 72 Geo. Wash. L. Rev. 1208, 1209-25 (2004) (summarizing the privacy protections of the Stored Communications Act). The states are free to impose greater restrictions on state and local officers. The Court should not short-circuit this active and dynamic legislative process by imposing a one-size-fits-all constitutional rule. *See Riley*, 134 S. Ct. at 2497-98 (Alito, J., concurring in the judgment).

Legislators certainly recognize the need for some kind of statutory privacy protection limiting government access to cell-site records. Everybody gets that. The real debate is over what standards and remedies should govern. In 1994, Congress amended the Stored Communications Act to impose a new "specific and articulable facts" standard for access to non-content historical network account records that include cell-site records. *See* Pub. L. No. 103-414, Title II, § 207(a) (1994). At the time, amicus curiae Electronic Frontier Foundation celebrated the new privacy law as a "critical" measure that achieved "a significantly greater level of protection" than traditional network privacy laws. *See* EFF Statement on and Analysis of Digital Telephony Act, October 8, 1994.[6]

Since 1994, Congress has frequently debated whether to further raise the statutory standard for access to cell-site records. By my count, the House Judiciary Committee and its subcommittees have held

---

[6] https://w2.eff.org/Privacy/Surveillance/CALEA/digtel94_passage_statement.eff

hearings partly or largely about this question five different times – in 2000, 2010 (twice), 2012, and 2013.[7] Committee Chair Robert Goodlatte promised last year that more legislative attention was coming. *See* Berin Szóka, *Privacy Reform Finally Moves in House: Goodlatte Promises Geolocation Privacy Bill Will Move Soon*,[8] Tech Policy Corner, Apr. 14, 2016.

State legislatures have also been active. California recently enacted the most far-reaching statutory privacy protection for network and electronic communications ever seen in the United States. *See generally* Susan Freiwald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA)*, Berkeley Tech. L.J. (forthcoming 2018).[9] Starting in 2016, the law not only requires a warrant for California law enforcement access to non-content records, including historical cell-site data, but it also imposes special particularity and nondisclosure rules for those warrants. *See* Cal. Penal Code § 1546(d), § 1546.1(b)(1), § 1546.1(d).

---

[7] The published reports of these hearings are available here:

bit.ly/HouseReport2000

bit.ly/HouseReport20101

bit.ly/HouseReport20102

bit.ly/HouseReport2012

bit.ly/HouseReport2013

[8] https://techpolicycorner.org/email-privacy-reform-finally-moves-in-house-df8f09962de6

[9] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2939412

III. THE COURT SHOULD REJECT CARPENTER'S MOSAIC THEORY OF THE FOURTH AMENDMENT.

Carpenter chiefly argues that the Court should follow the concurring opinions in *United States v. Jones*, 565 U.S. 400 (2012), which suggested that certain kinds of long term surveillance can become a Fourth Amendment search. Petr. Br. at 14-32. The *Jones* concurring opinions reflect the so-called "mosaic theory," by which government evidence-collection is not a search in isolation but becomes a search when aggregated and analyzed over some period of time to create a mosaic picture of a person's activities. *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311 (2012) (hereinafter *Mosaic Theory*).

A majority opinion of the Court has never adopted the mosaic theory. And it should not start now. The mosaic approach is well-intentioned but deeply misguided. It is a dramatic departure from traditional approaches, and it would drag state and federal courts into impossible line-drawing exercises that would cause endless confusion. Adopting the mosaic theory "would keep defendants and judges guessing for years to come," *Riley*, 134 S. Ct. at 2493, instead of providing the bright-line rules that are "essential to guide police officers." *New York v. Belton*, 453 U.S. 454, 458 (1981) (quoting *Dunaway v. New York*, 442 U.S. 200, 213-14 (1979)).

Before discussing the problems with the mosaic theory, it's important to realize that the *Jones* concurrences themselves suggest it may not apply to collection of historical cell-site records. Both concurrences in *Jones* were premised at least in part on the absence of legislation limiting the executive branch. *See Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (suggesting that the appropriateness of permitting executive discretion should be considered "in the absence of any oversight from a coordinate branch"); *id.* at 430 (Alito, J., concurring in the judgment) (justifying the approach because legislatures "have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes"). As discussed above, the collection of historical cell-site records is the subject of extensive statutory regulation at both the federal and state levels. The *Jones* concurrences are distinguishable on that basis alone.

If the Court must address the general viability of the mosaic theory, the approach should be rejected. Under the "longer term" aggregation approach advocated by Carpenter, the basic operation of Fourth Amendment doctrine would be thrown into doubt. The Court would need to answer an extensive list of novel and difficult questions to allow lower courts to implement the short-term/long-term distinction. In effect, the Court would need to create a parallel set of new Fourth Amendment rules. This would be a remarkable challenge. The Court should not adopt the mosaic approach without recognizing the complexities ahead.

I elaborate on the difficult questions in my *Mosaic Theory* article, *see id.* at 328-43, but here is an overview of the main questions. First, which surveillance methods are covered by a mosaic approach? If the mosaic theory applies to collection of historical cell-site records, does it also apply to collecting credit card records? Bank records? Use of automatic license plate readers? Use of public cameras installed by the government? Collection of camera footage from cameras installed by private actors? Monitoring of phone numbers dialed or Internet Protocol addresses used? Visual surveillance? Does the mosaic approach apply only to collecting location information, or does it apply to collecting any information – and if it is limited to location records, what about records (such as credit card statements) that permit plausible guesses about a person's location? Each technique, and many more, would need to be classified as included or excluded.

For each technique covered by the mosaic theory, a host of questions would arise. The most obvious – how long counts as "longer term" – is just the tip of the iceberg. Other questions include: Is the time period the same for different surveillance methods covered by the mosaic approach? What if several people used the device and no mosaic for any one individual can be constructed? And imagine the government uses two surveillance methods at the same time, such as GPS and cell-site tracking together, to monitor a suspect. Does that cut the window of allowed monitoring in half?

It gets even more complicated. Imagine the Court tries to draw a bright-line rule. Let's imagine, for the sake of argument, that 21 days of surveillance always triggers a mosaic search. Does switching surveillance methods restart the clock? For example, can the police do 20 days of GPS tracking, then 20 days of cell-site monitoring, and then 20 days of Internet Protocol address monitoring? Or does each day of any surveillance method count towards the 21-day total?

And is there a statute of limitations that resets the clock? Imagine investigators collect 20 days of cell-site records to avoid a search. Can they wait six months – or a year or two – and then get another 20 days' worth? And what if they get records only covering four hours per day, say, from 1pm to 5pm every day. Can they still only get records for 21 individual days before triggering a search, or can they now get records for up to 126 days because they are only collecting records for part of each day? And consider how the test works if there are multiple investigations of the same suspect, such as a federal investigation and a local investigation operating concurrently. Does the 21-day rule apply to all investigators collectively, or does separation among investigations mean different 21-day clocks?

Next consider how to determine the reasonableness of a mosaic search and what remedies apply to violations. Is a warrant required? If so, how can a mosaic warrant satisfy the particularity requirement when it is inherently about aggregating surveillance

from many places over time? If no warrant is required, how much cause is required? Do all mosaic searches require the same amount of cause, or do different mosaic techniques for time periods trigger different levels? What is the test for standing to challenge a mosaic search? Does the exclusionary rule apply, and if so does it apply to the entire surveillance that occurred or only that which crossed the line into being a search?

Carpenter offers no answers to these questions. "When the time comes to provide precise guidance to law enforcement agents and lower courts," Carpenter writes, "this Court will have ample authority to do so." Petr. Br. at 30. Carpenter won't even touch the simplest question of how long is "longer term." In some future case, Carpenter says, the Court can "set bright-line durational limits." *Id.* at 31. Just adopt the theory now, in other words. You can confront the maddening implications of it later.

The Court should decline this invitation. Fourth Amendment law requires certainty, *see Belton*, 453 U.S. at 458, in part because the blunt instrument of the exclusionary rule may apply. Because the government can lose its case if officers break the law, courts must provide clear rules that enable investigators to steer clear of violations. It is hard to see how courts can supply those clear answers under a mosaic theory. The many questions it raises "would keep defendants and

judges" – and for that matter, law professors – "guessing for years to come." *Riley*, 134 S. Ct. at 2493.[10]

IV. WHETHER REASONABLE PEOPLE EXPECT PRIVACY IN CELL-SITE RECORDS IS IRRELEVANT, AS THE THIRD PARTY DOCTRINE IS ABOUT MANIFESTING SUBJECTIVE EXPECTATIONS OF PRIVACY.

The parties frame this case as being largely about the reasonable expectation of privacy test. That test has been the subject of extraordinary confusion. Both courts and commentators have been unsure of what makes an expectation of privacy "reasonable." The uncertainty is understandable. The Court has mixed and matched among four different frameworks that offer different answers to what makes an expectation of privacy reasonable. *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan. L. Rev. 503 (2007). I have called these four frameworks the probabilistic, private facts, positive law, and policy models. *See id.* at 507-24. A close read of Carpenter's brief reveals rotating use of each of the four models. *See* Petr. Br. at 14-15 (probabilistic model); *id.* at 15-21 (policy

---

[10] For this reason, if the Court concludes that the Fourth Amendment governs government collection of historical cell-site records, the same Fourth Amendment restriction should apply to both short-term and long-term records collection. In that event, the Court should also conclude that the intermediate standard of 18 U.S.C. § 2703(d) satisfies the Fourth Amendment. *See* Resp. Br. at 50-55.

model); *id.* at 21-23 (positive law model); *id.* at 24-29 (private facts model).

Fortunately, the Court can and should sidestep the morass of the reasonable expectation of privacy test in this case. Properly understood, this case is not about the reasonable expectation of privacy test at all. Instead, like other cases concerning the third-party doctrine, it is actually about the subjective expectation of privacy test. *See* Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. Chi. L. Rev. 113, 115, 127-29 (2015) (hereinafter *Subjective Expectations*). From this perspective, Carpenter's position attempts to eliminate the original intended role of the subjective prong of the two-part *Katz* test that the Court has adopted. *See id.* at 115. The Court should reject Carpenter's invitation to set the Fourth Amendment on that new and uncharted path.

Appreciating this point requires a close read of Justice Harlan's famous concurring opinion in *Katz*. At the time of *Katz*, there were two distinct sets of Fourth Amendment precedents on what is a search. One set identified the spaces that could be the subject of Fourth Amendment protection. *See, e.g.*, *Rios v. United States*, 364 U.S. 253 (1960) (taxi cab); *United States v. Jeffers*, 342 U.S. 48, 51-52 (1951) (hotel room). *But see Hester v. United States*, 265 U.S. 57, 59 (1924) (open fields). The second set considered when a person waived protection in an otherwise-protected space by voluntarily revealing information to others such as undercover agents. *See, e.g.*, *Hoffa v. United States*, 385 U.S. 293, 302 (1966); *Lewis v. United States*, 385 U.S.

206, 210-11 (1966); *Osborn v. United States*, 385 U.S. 323, 325-27 (1966); *Lopez v. United States*, 373 U.S. 427, 438-39 (1963); *On Lee v. United States*, 343 U.S. 747, 749 (1952).

Justice Harlan's two-part *Katz* test simply summarized that case law. The "twofold requirement" was Justice Harlan's "understanding of the rule that has emerged from prior decisions" that explained how the Fourth Amendment protected a "place." *Katz*, 389 U.S. at 360 (Harlan, J., concurring). One requirement was that the government intrusion of a protected area be "a place" about which "society is prepared to recognize" an "expectation of privacy" as "reasonable." *Id.* This answered what spaces could be constitutionally protected. Conversation in homes and enclosed phone booths could be protected but "conversations in the open would not be protected." *Id.* at 360-61.

Another requirement was that a person must "have exhibited an actual (subjective) expectation of privacy." *Id.* at 361. Under this requirement, "objects, activities, or statements that he exposes to the plain view of outsiders" from inside a constitutionally protected space "are not protected because no intention to keep them to himself has been exhibited." *Id.* This accurately summarized the many cases holding that a person had no Fourth Amendment protection against the use of undercover agents even inside the home. *See, e.g.*, *Hoffa*, 385 U.S. at 302-03. The key was that an expectation of privacy had to be "exhibited," that is, demonstrated by an act. A person had to shield his speech from others to have protection; one who shared

information with others necessarily accepted the risk they would reveal it. *See id.*

All of this matters because *Carpenter* is about the second inquiry rather than the first. No one is characterizing the "place" where the cell-site records were obtained or stored. It is irrelevant whether "society is prepared to recognize" an expectation of privacy in that place as reasonable. This case instead is about cell-phone users' failure to exhibit a subjective expectation of privacy against a phone company's network connecting with the phone to route the user's communications. Using a phone that seeks a connection with local networks does not exhibit an expectation of privacy in the fact of that connection. Properly understood, the reasonable expectation of privacy test has no bearing on the issues raised in this case.

As I detailed in a recent article, some precedents of this Court have confused this point. *See Subjective Expectations* at 124-26. The "subjective" prong of the *Katz* test was wrongly assumed to be truly subjective. This confusion led the Court to move the disclosure principle over to the objective part of the test under the label of the so-called third-party doctrine. *Id.* The result is a doctrinal oddity. The two-part *Katz* test has been reduced to one part, and the third-party doctrine that was originally the subjective part of *Katz* is now a special application of the objective part. *Id.* at 127-33. No wonder so many scholars criticize the third-party doctrine: It comes off as a strange application of the reasonable expectation of privacy test. But that's because it's not an application of that test at all. The

Court should retain the third-party doctrine but characterize it properly as the subjective test, recognizing that it is distinct from the reasonable expectation of privacy test.[11]

This background explains the inability of Carpenter and his amici to identify a clear rule to govern this case. Carpenter seeks to do something truly new. He wants to introduce a right to stop others (here, cell phone companies) from disclosing to the government information he has shared with them. Carpenter can't identify a clear rule because no Fourth Amendment principle explains who can be stopped to talk about what they know and what facts they can't disclose. Any doctrinal line would be made out of thin air.

That poses no problem for legislatures. Legislatures can enact a nondisclosure rule that prohibits specific entities from disclosing specific kinds of information except pursuant to specific kinds of legal process. Congress has done exactly that in the Stored Communications Act. *See* 18 U.S.C. § 2702, § 2703. But it's hard to introduce a Fourth Amendment nondisclosure rule to determine what is a search. No constitutional text, history, or caselaw offers guidance on what

---

[11] In my *Subjective Expectations* article, I recommended eliminating the subjective prong while retaining the third-party doctrine. *See id.* at 133-34. I now think the more sensible approach is to restore the original understanding of *Katz* with the third-party doctrine properly labeled the subjective prong and distinguished from the objective prong.

such a private-party nondisclosure rule would look like.

The Empirical Scholars look for answers in public opinion polls and surveys. *See* Amicus Brief of Empirical Fourth Amendment Scholars at 2-10. They envision the *Katz* test as protection against the unexpected: Surprising disclosures to the government should require a warrant because they violate the expectations of ordinary people. *See id.* at 10-16. That has never been the law. "The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, *however well justified*, that certain facts will not come to the attention of the authorities." *United States v. Jacobsen*, 466 U.S. 109, 122 (1984) (emphasis added).

Nor should it become the law. The Constitution already includes an institution, Congress, that is designed to reflect public opinion about disclosures of information. It's also hard to see why the Fourth Amendment should protect against unexpected government action. And what disclosures are surprising to people is likely based on what they read on the Internet, which is not exactly a reliable basis for constitutional decisionmaking. Finally, it would be difficult for courts to implement a survey-based approach to what disclosures of information should be a search. Public opinion changes, and judges are not empiricists who are trained to compare and critique new scholarly research. Empirical studies can be useful in some contexts within Fourth Amendment law. But they cannot

Court should retain the third-party doctrine but characterize it properly as the subjective test, recognizing that it is distinct from the reasonable expectation of privacy test.[11]

This background explains the inability of Carpenter and his amici to identify a clear rule to govern this case. Carpenter seeks to do something truly new. He wants to introduce a right to stop others (here, cell phone companies) from disclosing to the government information he has shared with them. Carpenter can't identify a clear rule because no Fourth Amendment principle explains who can be stopped to talk about what they know and what facts they can't disclose. Any doctrinal line would be made out of thin air.

That poses no problem for legislatures. Legislatures can enact a nondisclosure rule that prohibits specific entities from disclosing specific kinds of information except pursuant to specific kinds of legal process. Congress has done exactly that in the Stored Communications Act. *See* 18 U.S.C. § 2702, § 2703. But it's hard to introduce a Fourth Amendment nondisclosure rule to determine what is a search. No constitutional text, history, or caselaw offers guidance on what

---

[11] In my *Subjective Expectations* article, I recommended eliminating the subjective prong while retaining the third-party doctrine. *See id.* at 133-34. I now think the more sensible approach is to restore the original understanding of *Katz* with the third-party doctrine properly labeled the subjective prong and distinguished from the objective prong.

such a private-party nondisclosure rule would look like.

The Empirical Scholars look for answers in public opinion polls and surveys. *See* Amicus Brief of Empirical Fourth Amendment Scholars at 2-10. They envision the *Katz* test as protection against the unexpected: Surprising disclosures to the government should require a warrant because they violate the expectations of ordinary people. *See id.* at 10-16. That has never been the law. "The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, *however well justified*, that certain facts will not come to the attention of the authorities." *United States v. Jacobsen*, 466 U.S. 109, 122 (1984) (emphasis added).

Nor should it become the law. The Constitution already includes an institution, Congress, that is designed to reflect public opinion about disclosures of information. It's also hard to see why the Fourth Amendment should protect against unexpected government action. And what disclosures are surprising to people is likely based on what they read on the Internet, which is not exactly a reliable basis for constitutional decisionmaking. Finally, it would be difficult for courts to implement a survey-based approach to what disclosures of information should be a search. Public opinion changes, and judges are not empiricists who are trained to compare and critique new scholarly research. Empirical studies can be useful in some contexts within Fourth Amendment law. But they cannot

provide the nondisclosure line-drawing that Carpenter needs.

V. THE ENACTMENT OF PRIVACY LEGISLATION DOES NOT GOVERN OR INFLUENCE THE MEANING OF THE FOURTH AMENDMENT.

Carpenter also argues that the enactment of privacy legislation should lead the Court to hold that he has Fourth Amendment rights in his cell-site records. He makes this argument in two ways. First, he argues that the existence of statutory privacy protections for cell-site records reflect a societal expectation of privacy in those records. Petr. Br. at 21-23. Second, he argues that designations found in 47 U.S.C. § 222 create a proprietary interest that makes cell-site records the user's constitutional "papers" or "effects." Petr. Br. at 32-35.

Both arguments should be rejected.

(a) Privacy Legislation Does Not Provide Evidence of Reasonable Expectations of Privacy.

The enactment of privacy legislation cannot bolster Carpenter's case for constitutional protection for two reasons. The first reason is implicit in the discussion above: Because this case *is* properly understood as being about a failure to manifest a subjective expectation of privacy rather than reasonable expectations of privacy, whatever reasonable expectations may exist are not relevant. *See* Part IV, *supra*. The second reason

is broader and more fundamental. Even if you assume that this is a case about reasonable expectations of privacy, privacy legislation cannot provide a helpful guide to assessing those expectations.

Here are the basic problems, drawing from a recent article that explores the issue in greater depth. *See* Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, 115 Mich. L. Rev. 1117 (2017) (hereinafter *Effect of Legislation*). First, privacy legislation does not signal Fourth Amendment values because it answers a very different set of questions. Any legal regime regulating law enforcement access must address three questions: What information is covered, how much protection is given to what is protected, and what remedies apply to violations. Because legislative privacy laws typically answer all three questions differently from Fourth Amendment law, one can't isolate any specific answer and imagine it sheds light on the constitutional framework when the two other answers are different. *Id.* at 1140-44.

The Stored Communications Act offers an example. Although the federal statute protects cell-site records from disclosure, that protection offers no guidance on whether the Fourth Amendment should do so. The statute imposes no limit on the scope of records obtained; it uses a "specific and articulable facts" disclosure standard; and it rejects a statutory exclusionary rule. Pet. App. 17a-18a. It's not clear how the coverage of the statute can inform a judgment about whether the Fourth Amendment should apply given that the

Fourth Amendment typically has a different scope, a different standard, and different remedies. *See Effect of Legislation* at 1140-44.

The same is true with state laws that adopt a warrant requirement for access to historical cell-site records. Even assuming the exclusionary rule applies to violations of those statutes, the states only have the constitutional authority to regulate state and local governments. Under the Supremacy Clause, state laws cannot regulate federal investigations. *See, e.g.*, *United States v. Supreme Court of N.M.*, 839 F.3d 888 (10th Cir. 2016). This makes it difficult to determine the lesson of a state law warrant requirement. Does it signal a wish to impose strong protection against disclosure of cell-site records, or does it signal only a wish to regulate collection by state and local officers? *See Effect of Legislation* at 1144-47.

Further, if the adoption of warrant-based protections by a minority of states signals something about the Fourth Amendment, what should we make of the fact that a majority of states have not enacted such protections? Does that mean most states see no privacy implications in the disclosure of cell-site data? That most states are fine with the federal standard? That most states just haven't yet reached the question? Looking at state laws for insights about privacy expectations requires drawing lessons from very mixed signals. Like mining legislative history for helpful comments, it is akin to "looking over a crowd and picking out your friends." Patricia M. Wald, *Some Observations on the Use of Legislative History in the 1981 Supreme*

Court Term, 68 Iowa L. Rev. 195, 214 (1983) (quoting Judge Harold Leventhal). The better approach is to interpret the Fourth Amendment independently of statutory privacy protections. *See Effect of Legislation* at 1157-64.

(b) 47 U.S.C. § 222 Does Not Make Cell-Site Records the User's Fourth Amendment "Papers".

Carpenter's argument that 47 U.S.C. § 222 makes cell-site records the customer's Fourth Amendment "papers" should also be rejected. To be sure, the Fourth Amendment concept of "papers" includes papers in electronic form. *See Katz*, 389 U.S. at 362 (Harlan, J., concurring); *United States v. Ackerman*, 831 F.3d 1292, 1304 (10th Cir. 2016) (Gorsuch, J.). At the same time, the Fourth Amendment only provides a right to persons in "their" papers, not in the papers of someone else. U.S. Const. Amend. IV; *Minnesota v. Carter*, 525 U.S. 83, 92-97 (1998) (Scalia, J., concurring).

The cell-site records collected in this case were the "papers" of the phone companies, not Carpenter. Cell-site records are information that a company creates, and a company then decides to store on its computers, about how the company's network was used. Users have no legal right to access their cell-site records. The records belong to the companies not their users. *Cf. id.* (Scalia, J., concurring).

Carpenter's argument to the contrary is based on 47 U.S.C. § 222, which imposes certain limitations on

the disclosure of customer-related records. The problem is that rules regulating disclosure do not create a property right in the regulated facts that belong to the subject of the disclosure. Confidentiality is not property. The fact that information concerns someone does not make that information his stuff. If the law limits when Alice can tell the world about what she saw Bob do, Alice's recollection does not become Bob's "papers" or "effects." Alice's recollections belong to Alice, not Bob. *Cf.* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 Stan. L. Rev. 1049, 1063-81 (2000).

CONCLUSION

The judgment of the court of appeals should be affirmed.

Respectfully submitted,

ORIN S. KERR
Counsel of Record
2000 H Street, NW
Washington, DC 20052
(202) 994-4775
okerr@law.gwu.edu

October 2, 2017

RECORD AND BRIEFS

No. 16-402

Supreme Court, U.S.
FILED
SEP 2 - 2017
OFFICE OF THE CLERK

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Sixth Circuit

AMICUS CURIAE BRIEF FOR NATIONAL DISTRICT ATTORNEYS ASSOCIATION IN SUPPORT OF RESPONDENT

Nelson O. Bunn, Jr.
Acting Executive Director
NATIONAL DISTRICT ATTORNEYS ASSOCIATION
Amicus Curiae
1400 Crystal Drive, Suite 330
Arlington, Virginia 22202
703-519-1666
nbunn@ndaajustice.org

John M. Castellano
Counsel of Record
125-01 Queens Boulevard
Kew Gardens, New York 11415
718-286-5801
jmcastellano@queensda.org

Linda Cantoni
Karen J. Friedman
Of Counsel

October 2, 2017

TABLE OF CONTENTS

Page No.

TABLE OF AUTHORITIES iii

STATEMENT OF INTEREST 1

SUMMARY OF ARGUMENT 1

CSLI RECORDS AND THEIR INVESTIGATIVE USES 4

ARGUMENT

I. Cell Phone Users Have No Cognizable Fourth Amendment Interest in Records Created and Maintained by Third-Party Carriers about the Routing of Communications through Their Networks 6

II. Petitioner's and Amici's Arguments Fail to Establish That He Had a Property Interest or a Reasonable Expectation of Privacy in His Carrier's Records Sufficient to Invoke the Fourth Amendment 11

A. Petitioner Has No Cognizable Property Interest in His Carrier's Records 11

B. The "Sensitive" Nature of the Information Held by Third Parties Does Not Alone Create a Reasonable Expectation of Privacy 12

C. Petitioner Has Not Shown That He Acted Involuntarily in Providing CSLI 16

D. Petitioner's Argument That He Reasonably Expected that His Information Would Not Be Disclosed to Law Enforcement is Unavailing 17

E. Petitioner's Attempt to Raise the Specter of Unrestrained Privacy Violations Is Unfounded 18

F. Petitioner's Position Would Require Overturning the Third-Party Doctrine, Thereby Dangerously Altering the Balance of Public and Private Interest in the Fourth Amendment 21

III. Even Assuming There Were a Cognizable Fourth Amendment Interest in CSLI, Court Orders Under Section 2703(d) Would Satisfy the Fourth Amendment 29

CONCLUSION 32

TABLE OF AUTHORITIES

Cases

Branzberg v. Hayes, 408 U.S. 665 (1972) 25

Burrows v. Superior Court, 13 Cal.3d 238 (1974) 14

California Bankers Ass'n v. Shultz, 416 U.S. 21 (1974) 23

California v. Carney, 471 U.S. 386 (1985) 29

Camara v. Mun. Court, 387 U.S. 523 (1967) 23

City of Ontario v. Quon, 560 U.S. 746 (2010) 27, 29

Couch v. United States, 409 U.S. 322 (1973) 22, 30

Donaldson v. United States, 400 U.S. 517 (1971) 7, 22

Ex parte Jackson, 96 U.S. 727 (1878) 10

Fisher v. United States, 425 U.S. 391 (1976) 7

Hale v. Henkel, 201 U.S. 43 (1906) 25

In re Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) 25

Katz v. United States, 389 U.S. 347 (1967) 6

McDonald v. United States, 335 U.S. 451 (1948) 31

NASA v. Nelson, 562 US 134 (2011) 29

Oklahoma Press Pub. Co. v. Walling,
327 U.S. 186 (1946) 23, 30

Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co., 593 F.2d 1030
(D.C. Cir. 1978) 26

Riley v. California, 134 S.Ct. 2473 (2014) 21

Smith v. Maryland, 442 U.S. 735
(1979) ..... passim

Terry v. Ohio, 392 U.S. 1 (1968) 30

United States v. Carpenter, 819 F.3d 880
(6th Cir. 2016) 4-5 n.2

United States v. Graham, 824 F.3d 421
(4th Cir. 2016) 18, 21

United States v. Jones, 565 U.S. 400 (2012) .. passim

United States v. Knights, 534 U.S. 112
(2001) 30

United States v. Miller, 425 U.S. 435
(1976) ..... passim

United States v. R. Enterprises, Inc.,
498 U.S. 292, 297 (1991) 27

United States v. Warshak, 631 F.3d 266
(6th Cir. 2010) 19-20

United States v. White, 401 U.S. 745
(1971) 7, 13

Wilson v. United States, 221 U.S. 361
(1911) 12

Constitution and Statutes

U.S. Const. amend IV ..... passim

18 U.S.C. § 2703 ..... passim

The Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, §§ 1100-22, 92 Stat. 3697-710 (1978) 28n.19

Other Authorities

2017 *Hiscox Embezzlement Study* (Aug. 17, 2017) (available at www.hiscox.com/2017-hiscox-embezzlement-study.pdf) 24 n.13

Boylan, *D., Military, Intelligence Agencies Alarmed by Surge in Bitcoin Value in 'Dark Web' Fight*, Washington Times (August 10, 2017) 24 n.14

Castellano, J., *Justices Poised to Consider, or Reconsider, Fourth Amendment Doctrines*, SCOTUSBlog www.scotusblog.com/2017/08/symposium-justices-poised-consider-reconsider-fourth-amendment-doctrines-assess-scope-privacy-digital-age (Aug. 1, 2017). 19 n.10

Eckenwiler, M., Prepared Statement, Hearing on Geolocational Privacy before the Subcommittee on Crime, Terrorism, Homeland Security and Investigations, No. 111-34 at 11 (April 25, 2013) 4 n.4

Ellis, B., *Identity Fraud Hits New Victim Every Two Second*, CNN Money (Feb. 6, 2014) 24 n.12

FBI, 2016 Internet Crime Report
https://pdf.ic3.gov/
2016_IC3Report.pdf 25 n.16

FBI, Insurance Fraud Statistics,
www.fbi .gov/stats-services/
publications/insurance-fraud 24 n.11

Fierce Wireless, *How Verizon, AT&T, T-Mobile, Sprint and More Stacked Up in Q2 2016* (Aug. 15, 2016) 19 n.9

Hearing Before the House Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, No. 113-34
(April 2013) 28 n.18

How Big Is a City Block?
www.land4ever.com/block.htm 4 n.2

Johnson, S., Dictionary of the English Language (1802) 12 n.7

Kerr, O., *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561 27

Kerr, O., *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801 (2004) 28

Kersey, J., A New English Dictionary (1702) 12 n.7

Modaferri, P., Testimony of International Association of Chiefs of Police, Hearing on Geolocational Privacy, n. 4, at 19-20, 23 ..... 5 n.5

Our Letters, N.Y. Times, Dec. 12, 1872 10

Parascandola, R., *Judge Sheila Abdus-Salaam Captured Nine Times on Video Before Suspicious Death,* NY Daily News (April, 28, 2017) 26 n.17

Staff Report, U.S. Senate, Permanent Subcommittee on Investigations, *Backpage.com's Knowing Facilitation of Online Sex Trafficking* (Jan. 9, 2017) (available at www.hsgac.senate.gov/ subcommittees /investigations /reports) 25 n.15

Statista, *Number of Monthly Active What's App Users*, www.statista.com/statistics/260819/ number-of-monthly-active-whatsapp-users 17 n.8

Sheridan, T., Dictionary of the English Language (1780) 12 n.7

Verison Full Privacy Policy 2017 ..... 9 n.6

Verizon Transparency Report, First Half, 2017 ..... 10 n.6

WhatsApp, Making Voice Calls, 2017, https://faq.whatsapp.com/en/android/ 28000016 ..... 17 n.8

STATEMENT OF INTEREST[1]

The National District Attorneys Association is the largest association of prosecuting attorneys in the country, representing 2,500 elected and appointed District Attorneys across the United States, as well as 40,000 Assistant District Attorneys. NDAA provides professional guidance and support, serves as a resource and education center, and follows and addresses criminal justice issues of national importance.

As active prosecuting attorneys, NDAA and its members are uniquely knowledgeable about the important investigative uses of cell site location information in state prosecutions, including developing probable cause, verifying information provided to law enforcement, and dispelling suspicion where it is unwarranted. In addition, members regularly use grand jury subpoenas to obtain third-party business records to advance their investigations of public corruption, identity theft, stalking, economic fraud, technology crimes, and countless other offenses · investigations that would be seriously threatened if the third-party doctrine were eliminated or heavily restricted, as amici and petitioner suggest.

SUMMARY OF ARGUMENT

In the course of investigating a four-month-long string of armed robberies in Detroit, prosecutors obtained three separate court orders under section 2703(d) of the Stored Communications Act for historical cell site location information (CSLI) – records created and maintained by wireless telecommunications providers reflecting the location of the carriers' cell towers used to route phone calls made and received by petitioner. The CSLI, collected by the

---

[1]No counsel for a party authored this brief in whole or in part, and no entity or person other than amici and their counsel made a monetary contribution intended to fund the preparation or submission of this brief. Both parties have granted blanket consent to amicus filings.

carriers for their own business purposes, placed petitioner's cell phone within one-half to two miles from the specified tower and within a 60 or120 degree radial wedge at the time of a call, covering from 35 city blocks to an area 28 times that large.

The government's actions in obtaining this information did not violate the Fourth Amendment. The orders did not direct a search or seizure of petitioner himself, his home, any paper he created, maintained or possessed, or any other of his physical effects.

Nor did petitioner have any reasonable expectation of privacy in the CSLI. The records and data were created and maintained by the carriers concerning their own infrastructure for their own business purposes; the data consisted purely of routing information, not content; and he himself relinquished the information when he used the carrier's network knowing, through his carrier's privacy policy, that this information was collected and could be provided to law enforcement. *See, e.g., Smith v. Maryland*, 442 U.S. 735 (1979) (no expectation of privacy in phone numbers dialed to route calls); *United States v. Miller*, 425 U.S. 435 (1976) (no expectation of privacy in financial information in bank records).

Petitioner contends, however, that this third-party information is his property, which the government could not seize without a warrant; that the information was highly sensitive, and therefore he had a reasonable expectation of privacy in it; and that he did not relinquish his information voluntarily because cell phones are an essential part of modern life. These objections are unavailing.

First, the property-based analysis of the Fourth Amendment aims to preserve the protections in existence at the time of the Amendment's passage, *see United States v. Jones*, 565 U.S. 400, 406 (2012), and petitioner provides no support for the proposition that

the framers would have understood information necessarily disclosed as part of a business transaction with a third party as protected property.

Second, CSLI is no more sensitive than other information that this Court has held is outside the Fourth Amendment when relinquished to a third party for a business purpose. Indeed, the precise numbers dialed by a phone customer are far more revealing as to her associations and affiliations than is her presence somewhere within an area covering many dozens of city blocks.

Similarly, when this Court decided *Smith*, landlines were considered just as indispensable a part of modern life as cell phones are now, providing essential business, social, and emergency uses. Yet this Court held that consumers' business transactions with the phone company were sufficiently voluntary to relinquish any privacy interest.

Moreover, this Court should not, as petitioner implicitly suggests and some amici explicitly avow, eliminate the third-party doctrine. To do so would preclude SEC and IRS summonses for financial information necessary for their functioning and would bring a halt to countless state prosecutions dependent upon review of third-party records, including public corruption, identity theft, insurance fraud, and stalking. It would also obstruct state grand juries from issuing document subpoenas for information necessary to their functioning.

Finally, even if there were an expectation of privacy in CSLI, it would undoubtedly be a diminished one, and the use of the SCA order here would be constitutionally reasonable. The statutory requirement of "specific and articulable facts" showing materiality and the necessity of prior judicial review and approval prevent the type of abuses petitioner predicts.

CSLI RECORDS AND THEIR INVESTIGATIVE USES

CSLI identifies the location of carriers' cell towers that are used in connecting customer calls and is generated, collected, and maintained by the carrier both for engineering reasons and for business purposes related to customer accounts. As noted above, in urban areas, cell towers are usually within one-half to two miles of the phone during the call, covering between 35 average-sized city blocks and an area 28 times that size,[2] but in rural areas, signals may extend as much as 20 miles (JA 47).[3]

The tower identified in these records need not have been the closest one to the phone, as network and environmental factors affect which tower is used to complete the call (JA 82-83). Even a call from a static location may switch towers in the middle of the conversation (JA 83), and two individuals riding in the same car may use two different towers to complete their calls. The records here, and those typically provided by carriers, do not reflect the use or existence of any cell signal equipment other than standard towers, such as "femtocells," "picocells," or "microcells" with smaller coverage areas.[4]

---

[2]The area covered encompasses 3.5 million to 100 million square feet, *United States v. Carpenter*, 819 F.3d 880, 889 (6th Cir. 2016), which converts to city blocks at an average rate of 100,000 square feet per block. *How Big Is a City Block?* www.land4ever.com/block.htm (accessed 9/26/2017).

[3]Numbers preceded by JA refer to the Joint Appendix and those preceded by PB to Petitioner's Brief.

[4]These "small cells" are often purchased by customers to expand access within a building or confined area, but do not expand the towers available to the general public and are generally not reflected in CSLI. Prepared Statement of Mark Eckenwiler, Hearing on Geolocational Privacy before the Subcommittee on Crime, Terrorism, Homeland Security and

CSLI does not reflect cell towers to which the phone connected while the phone was simply powered on, or cell towers used for the purpose of conveying any other data transmitted to or from the phone, such as for "apps" on a smart phone. Similarly, CSLI does not reflect GPS or other satellite-based data, or any real-time location information. Nor did law enforcement or the carriers involved in this case cause petitioner's phone to connect with the tower or otherwise seek out his location.

Orders for CSLI obtained under section 2703(d) have many important uses at the investigative stage of serious cases, either to build probable cause to obtain warrants or to dispel suspicions of those without blame. Investigators use available geolocation evidence as a filter to winnow out and prioritize leads from the unorganized mass of related and unrelated information that surrounds a crime and a crime scene.[5]

For example, where a case presents multiple suspects with strong motives to have committed a murder and possible access to the victim, CSLI may eliminate some or all of these individuals from suspicion by establishing they were elsewhere at the time of the crime.

CSLI may also be used to verify information provided by a confidential informant, helping law enforcement determine whether the information is reliable – an important showing in establishing probable cause and one that is required in some states. Similarly, CSLI can be used to corroborate or question the accounts of other witnesses, including some who

---

Investigations, No. 111-34 at 11 (April 25, 2013).

[5]Testimony of Peter Modaferri, International Association of Chiefs of Police, Hearing on Geolocational Privacy, *supra*, n. 4, at 19-20, 23.

are purporting to cooperate, but may be withholding critical information.

CSLI may also provide important clues in cases where homicide victims are found but little is known about the events leading up to their deaths. The victim cannot consent to the disclosure of the information, but CSLI may be critical in retracing the victim's steps and locating others who may have come in contact with the victim. Similar information may be important in determining the whereabouts of other non-communicative victims, such as those in a coma, and victims and witnesses who are frightened or reluctant to provide information, including domestic violence victims.

ARGUMENT

I. Cell Phone Users Have No Cognizable Fourth Amendment Interest in Records Created and Maintained by Third-Party Carriers about the Routing of Communications through Their Networks.

For most of our history, "the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates." *Jones*, 565 U.S. at 406. Added subsequently was the notion that government conduct obtaining access to an area or item in which the defendant had a legitimate expectation of privacy constituted a search under the Fourth Amendment, requiring that search to be reasonable. *See Katz v. United States*, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring). Applying these tests here, cell phone users can show neither a trespass upon protected areas nor a legitimate expectation of privacy in the records of wireless carriers.

The records here were created and maintained by wireless carriers, and contained data generated by and about their networks, which they had built and

maintained. Obtaining this information from the carrier did not require a search or seizure of petitioner's home or person, and the records were neither a paper nor effect of petitioner. Indeed, records of the operation of a business have for at least a century been considered outside the scope of the Fourth Amendment, as they are not papers or effects of the customer. *See Miller*, 425 U.S. at 440 ("the documents subpoenaed here [defendant's bank statements and copies of checks] are not respondent's 'private papers'. . . [R]espondent can assert neither ownership nor possession. Instead, these are the business records of the banks."); *Fisher v. United States*, 425 U.S. 391, 414 (1976) (accountants' workpapers and analyses not "private papers" of client); *Donaldson v. United States*, 400 U.S. 517, 522 (1971) (no Fourth Amendment issue in service of IRS summons on third party for financial records, "a question [that] appears to have been settled long ago"; citations omitted).

Similarly, wireless customers have no reasonable expectation of privacy in CSLI. First, the records contain information about the operation of the carrier, specifically the equipment and technology used to provide wireless services, and are generated for the carrier's own engineering and business purposes. A customer ordinarily has no expectation of privacy in records of how a business provides its services, such as how a power plant provides his electricity or where FedEx holds her packages. And while operational information may reflect certain facts about customer usage (the consumption of kilowatt hours at home or a penchant for sending flowers to a particular address), this information does not create a reasonable expectation of privacy in it. Indeed, the mere presence of information collected by another in the hands of a third party does not create a reasonable expectation of privacy in it, as a third party is ordinarily free to provide that information to the government and the government is free to seek it out. *United States v. White*, 401 U.S. 745, 749 (1971).

Second, to the extent that the carriers' records of the location of the cell towers a customer uses provides information about his location, he cannot claim a legitimate expectation of privacy, as he knowingly provides that information to the company in order to obtain its services.

Two seminal cases from this Court illustrate the principle. In *United States v. Miller*, 425 U.S. at 435, the government obtained by subpoena three months of defendant's bank statements and other financial records, including copies of individual deposit slips and checks. Defendant asserted an expectation of privacy in these records but this Court rejected the argument, reasoning that "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id.* at 442. The Court continued, "This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* at 443.

In *Smith v. Maryland*, 442 U.S. at 735, the Court held that the defendant had no "legitimate" expectation of privacy in the numbers he dialed on his home phone. The Court reasoned that phone customers "typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes." *Id.* at 743. According to the Court, knowledge of the phone company's ability to keep call records was evidenced by the detailing of long-distance numbers on their statements subject to a special rate structure, and the statements in phone books that companies "can frequently help in

identifying to the authorities the origin of unwelcome and troublesome calls." *Id.* Even though customers were required to convey the information to use the phone company's services, this Court concluded that the defendant "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed." *Id.* at 744.

Here, as in *Smith*, cellular customers who contract for and use services know, or reasonably should know, that their cell site location information is collected for business purposes and may be provided to law enforcement. Indeed, in making calls, customers know that they must be near a cell tower, or they cannot make a call. They must also be aware that the carrier knows the location of its own towers and that it has the capacity to collect and store that information. Indeed, if a customer wanders outside her home network, her phone tells her that she is roaming on another carrier's cell towers and subject to a special rate structure, just like the long-distance toll records in *Smith* alerted customers that the numbers they dialed were stored.

Thus, just as in *Smith*, wireless customers, by placing calls, convey the information necessary to complete the call and do so knowingly in order to obtain services. Indeed, here, petitioner had all the more reason to understand the risk he was assuming: carrier privacy policies explicitly state that this information will be provided to law enforcement upon the service of a subpoena or other legal process.[6] Just

---

[6] "Verizon, for example, specifically informs customers that it collects "wireless location" information and automatically monitors their connections, in part to "prevent our networks, services and users from fraudulent, abusive, or unlawful uses." Full Privacy Policy, Verizon, 2017. Verizon also advises customers that it "may

as phone customers could be expected to know information in their phone books in *Smith*, modern cell phone users should be expected to know information about their carriers' privacy policies. Indeed, wireless customers are required to acknowledge those policies at the time they enter into a contract as part of the terms of service, providing all the more reason they should know their contents.

Third, customers have no reasonable expectation of privacy in CSLI because it consists of only routing information, rather than the content of any communication. In the communications context, this Court has long drawn the distinction between information that is required in order to convey a communication and its content. Beginning with *Ex parte Jackson*, 96 U.S. 727, 733 (1878), this Court held that information required to deliver a communication, such as a physical address, is not constitutionally protected, even though it might bring embarrassment. "In a small village, for instance, a young gentleman may not altogether desire that all the loungers around the store which contains the Post-office shall be joking about the fair object of his affections." *Our Letters*, N.Y. Times, Dec. 12, 1872, at 4. Similarly, in *Katz* and *Smith*, this Court distinguished between the content of a call, which was protected, and the information necessary to complete it, which was not.

The location of the cell towers used to complete petitioner's calls unquestionably falls on the non-content side of that line. It is literally routing information – the route taken by the radio signals to complete petitioner's call. Nothing about the content

---

be required by law to disclose personally identifiable information to a governmental entity to comply with valid legal process, such as warrants, court orders or subpoenas." *Id.* In addition, Verizon's transparency reports specifically inform customers that location information is provided to law enforcement, including the precise number of requests. *See* Verizon Transparency Report, First Half, 2017.

of any call or message was disclosed, and the information was necessary to complete the call. It is, as this Court put it in *Smith*, "a means of establishing communication," not the communication itself. 442 U.S. at 741.

II. Petitioner's Arguments Fail to Establish that He Had a Property Interest or a Reasonable Expectation of Privacy in His Carrier's Records Sufficient to Invoke the Fourth Amendment.

A. Petitioner Has No Cognizable Property Interest in His Carrier's Records.

Petitioner argues that he has a property interest in the records because federal law generally limits its disclosure to others. This argument is flawed for several reasons. First, similar protections exist for bank records and for the numbers dialed on a telephone, yet petitioner does not dispute that these records remain outside the Fourth Amendment (PB 35).

Second, while Congress did enact protections for this information, it also expressly limited them by permitting disclosure of cell-site records in a variety of circumstances without a customer's consent, 47 U.S.C. 222(c)(1) and (d)(1)-(4), and by granting access to this very same information to the government upon a proper showing under the SCA. Petitioner cannot cite Congress's limited protections as creating a right and then transmogrify that limited right into an absolute right by assuming Fourth Amendment protection.

Third, the property-based Fourth Amendment analysis seeks to preserve the amount of privacy that existed at the time of the Amendment's passage, *see Jones*, 565 U.S. at 406, and it is highly doubtful that the founders would have believed that information they provided to others as part of a business transaction constituted their personal property.

Indeed, if a founder-era employee or independent contractor provided a detailed list of his travel and expenditures over a period of weeks or months to another for the purpose of obtaining reimbursement, it is unlikely he would believe this information constituted his property. Nor is there any evidence that a founding-era citizen would believe that information or records about the internal functioning of a business with whom he has contracted was somehow his property, or otherwise his "papers or effects."[7]

Indeed, if anything, the law at the time appears to have allowed third-party business records, which routinely convey information about transactions with customers, to be obtainable by subpoena, and therefore outside the Fourth Amendment's warrant requirement. *Wilson v. United States*, 221 U.S. 361, 373 (1911) (compelling compliance with subpoena *duces tecum* for corporate records and tracing its history to before the reign of Charles the Second).

B. The "Sensitive" Nature of the Information Held by Third Parties Does Not Alone Create a Reasonable Expectation of Privacy.

Petitioner and amici argue that customers have a reasonable expectation of privacy in CSLI because the information at issue is particularly sensitive and personal, and may reveal associational activities within the sphere of the First Amendment (PB 36-38). But even sensitive information conveyed to, or in the hands of, a third party, does not by itself give rise to a cognizable Fourth Amendment interest.

---

[7]In 1791, "effects" were defined merely as "goods" or "moveables." T. Sheridan, Dictionary of the English Language (1780); S. Johnson, Dictionary of the English Language (1802); J. Kersey, A New English Dictionary (1702) ("the Goods of a Merchant").

Indeed, even the most personal information trusted to a confidant could be disclosed to law enforcement when in the hands of a third party, including highly incriminating admissions. *United States v. White*, 401 U.S. at 749 ("however strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected by the Fourth Amendment when it turns out that the colleague is a government agent . . .").

The same applies to information provided to third parties in business transactions. Bank records contain what is generally considered to be highly private information, one's personal finances, which could reveal not only one's associations, but also precise dollar amounts conveyed to them, as well as the account holder's personal investments, donations to religious or charitable institutions, and the amount and purpose of loans and other credit. And the records obtained in *Miller* extended through three months of bank statements, potentially providing a telling picture of the defendant's associations, habits, and even opinions. Similar financial records could be even more revealing, such as credit card records, which provide a detailed list of where and when purchases are made.

Perhaps even more revealing are the phone numbers dialed from one's home. A record of phone calls made and received provide a detailed list of virtually all of one's associations – one far more precise than the wide-swath locational data conveyed by CSLI.

Yet, this Court specifically rejected arguments in *Miller* and *Smith* concerning the sensitive or confidential nature of the information at issue. In *Miller*, the Court upheld the disclosure of banking information over the dissent's objection that "in the course of his dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography." 425 U.S. at 451 (Brennan, J., dissenting). The *Miller* Court also

rejected the conclusions of *Burrows v. Superior Court*, 13 Cal.3d 238 (1974), quoted by the dissent, that depositors consider their information private and confidential, as two bank representatives had specifically testified in that case.

Petitioner, however, distinguishes the locational information at issue here, claiming it is far more private or confidential. He claims, in part, that locational data reaches into the home, an area specifically protected by the Fourth Amendment (PB 17-18). But this Court rejected the same contention in *Smith*, where the defendant argued that he demonstrated an expectation of privacy by his conduct because he used the telephone from his own house. As this Court explained, "the site of the call is immaterial for purposes of analysis in this case. . . . Regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call." 442 U.S. at 743. Thus, even assuming that the far less specific cell tower data here would be sufficient to place petitioner in his home, he necessarily conveyed that information in order to complete his call.

Petitioner nevertheless points to *United States v. Jones*, 565 U.S. at 406, as evidence that customers have an expectation of privacy in their location information, at least as aggregated over time. There are at least three critical differences, however, between *Jones* and this case. In *Jones*, the concurring justices expressed concern over satellite-based GPS location data, capable of pinpointing an individual's location to within 50 feet, because it "enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." 565 U.S. at 416.

By comparison, CSLI is far less revealing, quantitatively and qualitatively. Indeed, within the area covered by cell towers – between 35 city blocks and an expanse 28 times that large – an individual

could be at one of hundreds, if not thousands, of residences or businesses, precluding the reader from distinguishing between "a visit to a gynecologist, a psychiatrist, a bookie, or a priest," as petitioner contends (PB 17). And the more rural the locations, the greater the cell tower coverage, up to 20 miles. This lack of specificity is critical because CSLI does not provide the kind of associational information found troublesome by the concurrers, much less the ongoing detailed biography over time that so concerned them. *See Smith*, 442 U.S. at 742 (citing pen register's "limited capabilities" in determining that records of specific numbers dialed by defendant was not covered by Fourth Amendment). Indeed, CSLI, because of its lack of specificity, is never conclusive evidence on its own – it always has to be combined with other evidence to be meaningful, as it was in this case.

Nor does the assertion that other types of cell tower data could provide more specific information change the analysis (PB 27-28). No "microcells," "femtocells," or other small-range tower information was contained in the carriers' records here, and it ordinarily is not. Similarly, distances from the tower are not ordinarily calculated or reflected in CSLI. As this Court has noted, in interpreting the Fourth Amendment, it is important to specify the precise nature of the records obtained, rather than speculating about other technologies and their potential uses. *See Smith*, 442 U.S. at 741.

Second, unlike in *Jones*, here petitioner himself conveyed the location information to another as part of a business transaction to obtain specified services under circumstances where he either knew or should have known that this type of information was collected, and could be provided to law enforcement. While in *Jones*, the police surreptitiously planted a GPS device providing information directly to them, here petitioner knowingly provided the information to a third party as part of a business transaction in order to obtain a benefit. This Court's decisions in *Smith*, *Miller*, and

other cases preclude the finding that such information is private or protected under the Fourth Amendment.

C. Petitioner Has Not Shown That He Acted Involuntarily in Providing CSLI.

Petitioner and amici, however, argue that this case is distinguishable from *Miller* and *Smith* because customers do not "voluntarily" provide CSLI to their carriers. They argue that cell phone use is effectively compelled in modern society and that customers thus have no choice but to convey cell site location information (BP 35).

But in the pre-digital era, use of landline phones was considered just as essential, yet this Court held that the numbers dialed were not within the Fourth Amendment. Indeed, before cell phones, landline phones, in common use for many decades, were used for every facet of daily life, including social interaction, business transactions, and emergency services. Nor were there other readily-transmitted means of communication that are available now, like emails, making phones all the more essential then. The fact that phone service was an indispensable feature of virtually every home and that phone numbers had to be conveyed to obtain that service did not render the relinquishing of this information any less voluntary, in this Court's view.

Similarly, at the time *Miller* was decided, use of banking and personal credit services were an essential facet of everyday life, yet the information conveyed in order to obtain those services does not enjoy Fourth Amendment protection. And this Court so held in *Miller* despite the specific objection that, "[f]or all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account." 425 U.S. at 451.

Nor is it true, as petitioner contends, that he was unable to restrict the conveyance of his CSLI, even when at a sensitive location. Indeed, while the defendant's calls from his home in *Smith* necessarily required him to convey the numbers dialed, today's smart phone options allow users to minimize the provision of CSLI with little effort. Petitioner could have, for example, used any number of common smart phone applications to complete calls or otherwise confer with his friends or associates without providing CSLI.[8] And, of course, petitioner could have placed his phone on "airplane" mode, turned it off, or simply left it at home, in his car, or at any secure location. But he did none of these, suggesting his concern for locational privacy was simply not that great.

D. Petitioner's Argument That He Reasonably Expected that His Information Would Not Be Disclosed to Law Enforcement Is Unavailing.

Petitioner argues that even if he knew that the location of the cell towers used to complete his calls would be conveyed to the carrier, he still had a reasonable expectation that it would not be turned over to law enforcement. This argument is both counterfactual and foreclosed by *Smith* and *Miller*.

First, both *Smith* and *Miller* held that even though the defendants released their information to

---

[8]Universally available free applications like "WhatsApp?" and "Viber" provide the ability to text message and make and receive phone calls through internet connections that are not reflected in CSLI. *See, e.g.*, *WhatsApp. Making Voice Calls.* 2017. https://faq.whatsapp.com/en/android/28000016. Applications like "Skype" and "Facetime" use similar technology to permit audio and video calls and are not reflected in CSLI. Users of these applications number in the billions. *See, e.g.*, Statista. *Number of Monthly Active WhatsApp Users.* https://www.statista.com /statistics/260819/number-of- monthly-active-whatsapp-users (1.3 billion).

specific third parties, and might have expected confidentiality as to the government, the information was afforded no constitutional protection. *See Smith*, 442 U.S. at 744; *Miller*, 425 U.S. at 443.

Second, even if that argument were not foreclosed, cell phone users either know or should know of the specific risk that CSLI could be provided to law enforcement. Carriers' privacy policies, which customers are required to accept as a condition of receiving service, disclose that CSLI can be, and is, turned over to law enforcement upon proper legal process.

E. Petitioner's Attempt to Raise the Specter of Unrestrained Privacy Violations Is Unfounded.

Petitioner nevertheless warns that if the third-party doctrine is "extended" to CSLI, it will allow the government unrestrained access to every type of digital information, whether accessed on a cell phone or otherwise. He argues that police will have license to track every American at will, that his emails will be hacked by law enforcement, and that his most intimate opinions and thoughts will be collected by the government. Indeed, he speculates that there is already evidence of law enforcement's rampant abuse of CSLI.

This is simply not so. First, an affirmance here would not by itself permit "tracking" of citizens. Indeed, no real-time locational information is at issue, nor did prosecutors cause the company to send a signal or "ping" petitioner's phone to discern its location. *United States v. Graham*, 824 F.3d 421, 425-26 (4th Cir. 2016) (explaining that "[n]o government tracking is at issue here"). Moreover, the general historical information that was requested requires a court order under the SCA and thus cannot be acquired wholesale or mined by law enforcement.

Similarly, petitioner's and amici's allegations of abuse of CSLI are without foundation. While citing statistics from carriers' transparency reports on the numbers of requests made for such information, they make no effort to put those absolute numbers in context. For example, they do not compare the number of requests to the number of subscribers of the same company, much less the number of days of CSLI requested to the number of days subscribers used their phones. Moreover, even the roughest comparison belies petitioner's position. For example, Verizon's 53,532 requests, cited by the Electronic Frontier Foundation in their brief (p. 13-14), as compared to its more than 142 million subscribers[9] reveals that law enforcement obtains only the tiniest shard of this type of information – less than one-hundredth of a percentage point – hardly the dragnet so frequently alleged.[10] And the EFF makes no effort to compare the information to the number of subpoenas issued for bank records, numbers dialed, or other records obtainable by subpoena.

Moreover, lower courts applying the third-party doctrine have still thoughtfully afforded constitutional protections to a great variety of private data. Courts, for example, have adhered to the traditional distinction between content and conveyance of messages, ensuring that the contents of any email or text message will fall within the Fourth Amendment. *See, e.g., United States*

---

[9]Fierce Wireless, *How Verizon, AT&T, T-Mobile, Sprint and More Stacked Up in Q2 2016* (Aug. 15, 2016).

[10]Other evidence points to a restrained use. For example, in Queens, New York, the 10th most populous county in the nation with 2.3 million inhabitants and more than 54,000 prosecutions in 2016, prosecutors obtained CSLI orders only 92 times. Castellano, *Justices Poised to Consider, or Reconsider, Fourth Amendment Doctrines*, SCOTUSBlog http://www.scotusblog.com/2017/08/symposium-justices-poised-consider-reconsider-fourth-amendment-doctrines-assess-scope-privacy-digital-age (Aug. 1, 2017). More than half of these orders were for ten days or less, and only seven exceeded 90 days, mostly for pattern crimes. *Id.*

v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010). Social network pages are also ordinarily simply messages to a limited group of friends and thus protected substantive communications. And similar content-based distinctions could be made with regard to other types of digital information, including, for example, one's internet searches or other expressive information. In addition, images and documents stored digitally by third parties are readily analogized to other types of storage containers, like lockers, that are provided by third-party bailees and require a warrant to open.

True, a limited amount of information conveyed to third parties reflecting business transactions might be accessible to the government, upon a proper showing under the SCA. But this same business information would have been accessible before the advent of the digital age, including in the most robust economy when such transactions were abundant. In many, if not most, cases, it makes little difference whether information formally written in ledgers is now held digitally: the taxi dispatcher's written records of a customer's trip, including the timing and destination, are not so profoundly different from Uber's records of its customers' trips that the two situations demand different constitutional treatment.

And, to the extent that these business transactions have increased or that different types of information may be conveyed by the customer, most Americans understand that there is a necessary diminution of privacy in the digital era, and are willing to accept the tradeoff. *See Jones*, 565 U.S. at 427 (Alito, J., concurring) ("New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable").

This is not to say that individuals do not *desire* privacy, even as they release their information to others. But there is a distinction between desiring privacy and reasonably expecting it. As Judge Wilkinson wrote concurring in *United States v. Graham*, 824 F.3d at 441: "It is human nature, I recognize, to want it all. But a world of total privacy and perfect security no longer exists, if indeed it ever did."

Petitioner relies on *Riley v. California*, 134 S.Ct. 2473 (2014), to argue that doctrines from the pre-digital era cannot be woodenly applied to digital data. Neither can they be entirely ignored. Indeed, in *Riley*, this Court expressly referred to other exceptions to the warrant requirement that could apply to cell phones, or to some portion of the information in them. *Id.* at 2494. Here, CSLI falls squarely within the third-party doctrine and the well-established distinction between content and non-content applicable to communications. Moreover, the ability to access CSLI is far less intrusive than the virtually unlimited permission of law enforcement sought in *Riley* to scavenge through the wealth of information available on a modern smart phone. *Riley*, then, does not advance petitioner's argument.

F. Petitioner's Position Would Require Overturning the Third-Party Doctrine, Thereby Dangerously Altering the Balance of Public and Private Interest in the Fourth Amendment.

While petitioner attempts to distinguish *Miller* and *Smith*, these efforts fall short. *Miller* and *Smith* directly refute his arguments concerning the sensitivity of the information conveyed, the expectation that the information will not be provided to the government, and the idea that the data is entitled to protection as private papers or property. Nor can these cases be limited to their facts, as petitioner and some amici suggest.

Financial records are today created and maintained digitally and thus *Miller* would have no effect at all if limited to paper records. Nor can digital banking records be meaningfully distinguished from other information disclosed digitally in the course of business transactions. Similarly, the numbers dialed by phone users are collected digitally, and were contained on the very same document that petitioner's carriers provided here. It would indeed be anomalous if law enforcement could freely view the column of specific phone numbers contained in the carriers' records, but were precluded from seeing the location of the cell towers used to route the calls.

In short, in order to rule in favor of petitioner, this Court would have to abolish the third-party doctrine, a goal more candidly avowed by some amici than by petitioner. This conclusion belies petitioner's argument that all he seeks is the same degree of privacy he had before the advent of the digital age (PB 18); indeed, he is asking for far more, including unwarranted privacy in banking records, numbers dialed, his accountant's papers, and the myriad other forms of information conveyed to third-party businesses that previously would have been available by a subpoena *duces tecum*. The Court should reject petitioner's attempt to overturn this doctrine.

First, to do so would not only require overruling *Miller* and *Smith*, but also overturning cases extending back far earlier. This includes, for example, this Court's cases upholding document subpoenas directed to accountants and other businesses even though those subpoenas clearly disclosed information about clients. *See, e.g., Couch v. United States*, 409 U.S. 322, 336 n. 19 (1973) (accountant's client does not have "the necessary expectation of privacy to launch a valid Fourth Amendment claim" concerning seizure of accountant's records); *Donaldson v. United States*, 400 U.S. 517, 522 (1971) (upholding IRS summons to employer and employer's accountant and finding no constitutional issue; the question "appears to have been settled long

ago when the Court upheld, against Fourth Amendment challenge, an internal revenue summons issued under the Revenue Act of 1921 and directed to a third-party bank"); *Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 208 (1946) ("the Fourth [Amendment], if applicable, at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described . . .'"). *See also California Bankers Ass'n v. Shultz*, 416 U.S. 21, 53 (1974) (rejecting Fourth Amendment challenge to Bank Secrecy Act requirements: "(I)t is difficult to see how the summoning of a third party, and the records of a third party, can violate the rights of the taxpayer, even if a criminal prosecution is contemplated or in progress").

Second, eliminating the ability of prosecutors to obtain these types of documents would stymie many types of investigations currently dependent on business documents and thereby dangerously upset the existing balance between public and private interests under the Fourth Amendment. *Camara v. Mun. Court*, 387 U.S. 523, 534 (1967) (expressing that "accommodation between public need and individual rights is essential" in interpreting the Fourth Amendment). For example, subpoenas directed to accountants, routinely used in state and federal tax prosecutions, would be precluded because the information in the hands of the accountant would consist of personal financial records subject to the warrant requirement. Similarly, subpoenas issued to financial institutions in securities fraud investigations would no longer be valid, as probable cause and a warrant would be required.

The investigation of many other crimes routinely prosecuted by state district attorneys would also come to a halt because they are dependent on subpoenas of financial records or similar third-party documents. These subpoenas allow investigators to trace funds, confirm identities, and investigate myriad types of fraud and related crimes. Investigations dependent on these subpoenas include cases involving insurance fraud, identity theft, credit card fraud, mortgage fraud,

money laundering, embezzlement, elder fraud, and the defrauding of government benefit programs.

The effect of eliminating this investigative tool in such prosecutions is staggering. Insurance fraud causes 40 billion dollars worth of losses each year,[11] and identity theft has been estimated to strike a new victim every two seconds.[12] Embezzlement prosecutions, which create *average* losses for business and government agencies of well over one million dollars per year, and disproportionately affect smaller businesses, would also be seriously impeded.[13] Nor are the investigations affected solely those for economic crimes. Public corruption prosecutions focus on financial records to trace funds. stalking cases are often dependent on records of communications, and third-party records are used in countless other prosecutions for such ordinary matters as, for example, learning who rented a car observed at the scene of a crime.

Moreover, as society generally has become computerized, criminals actively use, and hide their crimes in, the digital maze. They use Bitcoins to conduct illicit business, hide proceeds, and launder money,[14] take advantage of the increased access presented by online forums to perpetrate their frauds against the young, the gullible, and the elderly, and use internet advertising to sell child sexual services and

---

[11]FBI, Insurance Fraud Statistics, https://www.fbi.gov/stats-services/publications/insurance-fraud (accessed 9/22/17).

[12]Ellis, *Identity Fraud Hits New Victim Every Two Seconds*, CNN Money (Feb. 6, 2014).

[13]2017 *Hiscox Embezzlement Study* (Aug. 17, 2017) (available at http://www.hiscox.com/2017-hiscox-embezzlement-study.pdf) (accessed 9/20/17).

[14]Boylan, *Military, Intelligence Agencies Alarmed by Surge in Bitcoin Value in 'Dark Web' Fight*, Washington Times (Aug. 10, 2017).

illicit wares.[15] They also use technology to commit crimes in other ways not previously possible, including ransomware and tech support fraud.[16] This explosion in internet crime would become immeasurably more difficult to combat with the elimination of the third-party doctrine, impeding law enforcement efforts to simply keep pace to investigate the same crimes it would previously prosecute. "Law enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system." *In re Historical Cell Site Data*, 724 F.3d 600, 614 (5th Cir. 2013).

Third, the abandonment of the third-party doctrine would also substantially limit the traditional power of state grand juries, which routinely issue document subpoenas in the course of their proceedings. Grand juries are an integral part of many state justice systems, and, particularly in economic crime and public corruption cases, conduct meaningful, long-term investigations into fraud and misconduct. Moreover, this Court has recognized that body's essential role and enforced its subpoenas even against First Amendment challenges. *Branzberg v. Hayes*, 408 U.S. 665 (1972). Nor was the Fourth Amendment previously seen to be incompatible with a properly issued grand jury subpoena *duces tecum* directed at a business, even though it might reflect on individual customers or officers. *Hale v. Henkel*, 201 U.S. 43, 73 (1906) ("We think it quite clear that the search and seizure clause of the Fourth Amendment was not intended to interfere with the power of courts to compel, through a subpoena

---

[15]Staff Report, US Senate Permanent Subcommittee on Investigations, *Backpage.com's Knowing Facilitation of Online Sex Trafficking* (Jan. 9, 2017) (available at https://www.hsgac.senate.gov/subcommittees/investigations/reports) (accessed 9/24/17).

[16]FBI, 2016 Internet Crime Report, at 10-11, https://pdf.ic3.gov/2016_IC3Report.pdf (accessed 9/26/17).

duces tecum, the production . . . of documentary evidence").

Fourth, the frequent criticism that the third-party doctrine misunderstands the voluntariness of the information provided to the third party should be rejected. Indeed, in some respects, information in the hands of third parties should be available to law enforcement regardless of whether it was disclosed voluntarily. If, for example, a wife hires a private investigator to follow her spouse and take notes of his comings and goings, the husband would have no standing to challenge the government's seizure of the notes, even though it contained his personal location information and even though he did not provide that information voluntarily. Similarly, an individual's location captured on a third party's private security camera, or even network of cameras,[17] may be conveyed "involuntarily" but a defendant would ordinarily have no standing to preclude a third party from releasing it.

Furthermore, the third-party doctrine's conception of voluntariness reflects a fundamental logic: "In any normal life, even in pursuing his most private purposes, the individual must occasionally transact business with other people. When he does so, he leaves behind, as evidence of his activity, the records and recollections of others. He cannot expect that these activities are his private affair." *Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co.*, 593 F.2d 1030, 1043 (D.C. Cir. 1978).

Fifth, the alternative theory – that information retains its private character even as it is released to

---

[17] Large apartment complexes, private universities, and sprawling corporate campuses often have networks of surveillance cameras, and, even in their absence, police frequently contact multiple third parties with surveillance capabilities to piece together an individual's movements over time. *See, e.g.*, *Judge Sheila Abdus-Salaam Captured Nine Times on Video Before Suspicious Death*, NY Daily News (April 28, 2017).

others or enters the stream of commerce – is fatally flawed as a constitutional doctrine. Initially, it would be impractical at best. For example, documents subpoenaed in the course of investigations of businesses could not be examined until the source of the information in the records was determined. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 581-82 (2009). Even then, law enforcement would presumably need probable cause to believe the individuals whose information is contained in the record committed a crime, a requirement this Court has rejected. *United States v. R. Enterprises, Inc.*, 498 U.S. 292, 297 (1991). The doctrine would also create other vexing questions, such as when otherwise personal information would lose its protection by being divulged to others on repeated occasions.

The alternative theory would also create other untenable results. For example, law enforcement would presumably be free to approach third parties for their oral recollections or knowledge of personal information about a defendant, including her business transactions, and grand juries could compel the attendance and testimony of such a witness, but could not obtain a written, and more precise, memorialization of that same transaction.

Moreover, as four concurring justices of this Court observed in *Jones*, "'[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." 565 U.S. at 429–30. *See City of Ontario v. Quon*, 560 U.S. 746, 759 (2010). Indeed, much of the purported social science data cited by amici would be far better presented and evaluated in legislative hearings, as would the countervailing needs of law enforcement to address criminal exploitation of

the internet.[18] There, statutory schemes can be debated, the impact of those proposals assessed by such impartial arbiters as the Congressional Budget Office, and representatives can fashion a nuanced remedy. The judicial response, by contrast, is confined to voting up or down on the specific, limited set of facts presented in particular litigation, often years or decades after the technological advances are in place. It also frequently results in circuit conflicts that ultimately require this Court to continually "update and redefine the Fourth Amendment as technology evolves" – a procedure ill-suited to technological advances that develop at breakneck speed. *See* Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 805 (2004).

Nor has Congress been inadequate to the task of creating statutory schemes to protect informational privacy, as it promptly did to regulate the privacy of banking records after *Miller*,[19] and as it has already done with regard to telecommunications and internet providers in the SCA. The statutes enacted include the precise mechanism used here, the section 2703(d) order, which balances privacy concerns and legitimate government needs by requiring pre-compliance judicial review and approval. Lower courts, including the Sixth Circuit here, have reasonably adopted that mechanism as a meaningful accommodation of interests. And, as

---

[18]The House, for example, has conducted hearings on geolocational privacy and how to address it, *see* Hearing before the House Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, No. 113-34 (April 2013), and the Senate has conducted an extensive investigation into the illicit operations of backpage.com and how to address them. *See* note 15, *supra*.

[19]*See* The Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, §§ 1100-22, 92 Stat. 3697-710 (1978).

detailed below, this conclusion presents a separate ground for affirmance here.[20]

III. Even Assuming There Were a Cognizable Fourth Amendment Interest in CSLI, Court Orders Under Section 2703(d) Would Satisfy the Fourth Amendment.

Even if this Court were to find that the petitioner had some expectation of privacy in CSLI, that expectation would necessarily be diminished for many of the reasons cited above. The 2703(d) order used here and by most prosecutors nationwide was adequate to address the concerns raised by that diminished expectation and render the government's conduct reasonable under the Fourth Amendment. Indeed, this Court may, as it has in the past, decide this case by assuming, without deciding, the existence of a cognizable interest, and finding the government conducted itself reasonably. *See NASA v. Nelson*, 562 U.S. 134, 147 (2011); *Quon*, 560 U.S. at 760. This could well be the easiest path here, and is far narrower and more certain in its scope than any ruling abolishing the well-established third-party doctrine.

Where government conduct intrudes on only a diminished expectation of privacy, this Court has on many occasions relaxed the warrant requirement, relying on the Fourth Amendment's more general command that citizens be free of "unreasonable" searches. These exceptions apply to, among other things, a person's diminished expectation of privacy in his automobile, *California v. Carney*, 471 U.S. 386, 391 (1985); the diminished expectation of privacy attendant

---

[20]In addition to finding that petitioner had no expectation of privacy in CSLI, the Sixth Circuit addressed the reasonableness of any cognizable intrusion under the Fourth Amendment, expressly rejecting the argument that the balance adopted by Congress in section 2703(d) was constitutionally inadequate. 819 F.3d at 889-90.

to a short detention rather than an arrest, *Terry v. Ohio*, 392 U.S. 1 (1968); and the diminished expectation of a probationer in his home and belongings, *United States v. Knights*, 534 U.S. 112 (2001).

In addition, this Court has held that the diminished expectation of privacy possessed by a business or corporation in its own books requires merely a subpoena, and this applies even where the records reflect information about clients or customers. *See, e.g., Couch v. United States*, 409 U.S. at 336 n. 19.

Here, even assuming a phone customer has some expectation of privacy in CSLI, that privacy interest would necessarily be diminished. This is for many reasons, including that location information is generally exposed to the public; CSLI discloses only the most general geographic areas and does not reveal specific locations or associations; CSLI consists of non-content routing information created and kept by a third party for its own business purposes; and customers relinquish the information after being informed that it is collected and may be disclosed to law enforcement.

The 2703(d) order reasonably addresses the concerns raised by these diminished expectations. The statutory provision requires a specification of the documents, a particularized showing of their relevance and materiality, and judicial intervention before the records are disclosed. Under 2703(d), law enforcement must demonstrate "specific and articulable facts" showing "reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." This required demonstration of materiality "guards against abuse . . . by way of too much indefiniteness or breadth." *Walling*, 327 U.S. at 208.

Even more importantly, the statute requires judicial intervention before compliance. This provides a critical element of the Fourth Amendment's protection because it "interpose[s] a magistrate between the

citizen and the police ... so that an objective mind might weigh the need to invade [the searchee's] privacy in order to enforce the law." *McDonald v. United States*, 335 U.S. 451, 455 (1948).

This mechanism also avoids the precise ill identified by petitioner and amici, the purported "dragnet" collection and storage of location information to be searched for any purpose whatsoever. It allows the court to review the required "specific and articulable facts," and ensure that the CSLI is relevant and material to specific crimes. And it allows the court to control not only access to CSLI in the first place but also to limit the quantity or duration of the information obtained since relevance and materiality will depend on the timing of the crimes being investigated.

CONCLUSION

Cell phone customers have no cognizable interest in carrier records identifying the towers used to route their calls, and the privacy of CSLI is nevertheless protected from government abuse by judicial intervention. The order of the Sixth Circuit should therefore be affirmed.

Respectfully submitted,

Nelson O. Bunn, Jr.
Acting Executive Director
NATIONAL DISTRICT ATTORNEYS ASSOCIATION
1400 Crystal Drive, Suite 330
Arlington, VA 22202
(703) 519-1666
nbunn@ndaajustice.org

John M. Castellano
Counsel of Record
125-01 Queens Boulevard
Kew Gardens, NY 11415
(718) 286-5801
jmcastellano@queensda.org

Linda Cantoni
Karen J. Friedman
Of Counsel

October 2, 2017

RECORD AND BRIEFS

Supreme Court, U.S.
FILED
AUG 14 2017
OFFICE OF THE CLERK

No. 16-402

IN THE
Supreme Court of the United States

TIMOTHY IVORY CARPENTER,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

On Writ of Certiorari to the
United States Court of Appeals for the Sixth Circuit

BRIEF *AMICI CURIAE* OF THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS AND 19 MEDIA ORGANIZATIONS IN SUPPORT OF PETITIONER

Bruce D. Brown
Counsel of Record
Caitlin Vogus
Selina MacLaren
THE REPORTERS COMMITTEE
FOR FREEDOM OF THE PRESS
1156 15th St. NW, Suite 1250
Washington, D.C. 20005
bbrown@rcfp.org
(202) 795-9300

Additional counsel listed in Appendix A

TABLE OF CONTENTS

TABLE OF CONTENTS i

INTEREST OF AMICI CURIAE 1

SUMMARY OF ARGUMENT 9

ARGUMENT 11

I. The history of the Fourth Amendment is intertwined with the First Amendment's guarantees of free expression and a free press. ... 11

II. Warrantless acquisition of CSLI records chills the exercise of First Amendment rights, including newsgathering. 14

A. Long-term tracking of historical CSLI can reveal sensitive First Amendment-protected activities. 15

B. CSLI acquisition threatens the newsgathering process. 17

III. Fourth Amendment protections should be rigorously applied when the government seeks to obtain CSLI because First Amendment interests are at stake. 22

IV. The U.S. Court of Appeals for the Sixth Circuit's application of the third-party doctrine to CSLI records imperils the free and unfettered exercise of First Amendment rights. 23

CONCLUSION 28

APPENDIX A: List of Additional Counsel A-1

TABLE OF AUTHORITIES

Cases

Bates v. Little Rock, 361 U.S. 516 (1960) 17

Boyd v. United States, 116 U.S. 616 (1886) . 11, 12, 13

Brower v. County of Inyo, 489 U.S. 593 (1989) 12

City of Ontario v. Quon, 560 U.S. 746 (2010). 15

Commonwealth v. Augustine, 4 N.E.3d 846 (2014) . 26

Entick v. Carrington, 19 How. St. Tr. 1029 (C.P. 1765) 11, 12

Frank v. Maryland, 359 U.S. 360 (1959) 14

In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to Gov't, 620 F.3d 304 (3d Cir. 2010) 24, 26

In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) 24

Kyllo v. United States, 533 U.S. 27 (2001) 25

Marcus v. Search Warrant, 367 U.S. 717 (1961) 11, 13

NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958) 16

Riley v. California, 134 S. Ct. 2473 (2014) 15, 20

Smith v. Maryland, 442 U.S. 735 (1979) 22, 24, 25

Stanford v. Texas, 379 U.S. 476 (1965) .....*passim*

State v. Earls, 70 A.3d 630 (N.J. 2013) 16

United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016) 24

United States v. Davis, 785 F.3d 498 (11th Cir. 2015) 24, 25

United States v. Forrester, 512 F.3d 500 (9th Cir. 2008) 26

United States v. Graham, 824 F.3d 421 (4th Cir. 2016) 15, 24, 25, 26

United States v. Jones, 565 U.S. 400 (2012) 16, 17, 27

United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) 16

United States v. Miller, 425 U.S. 435 (1976) 24

Wilkes v. Wood, 19 How. St. Tr. 1153 (C.P. 1763).. 11, 13

Zurcher v. Stanford Daily, 436 U.S. 547 (1978) .....*passim*

Statutes

18 U.S.C. § 2703(d) 19, 22

Other Authorities

Dan Gillmore, *Beyond Encryption*, Colum. J. Rev. (May 7, 2012)..... 21

Dana Priest, *CIA Holds Terror Suspects in Secret Prisons*, Wash. Post (Nov. 2, 2005) 19

Eric Lichtblau, *C.I.A. Tracked Russian Prying in the Summer*, N.Y. Times (Apr. 7, 2017)..... 19

FBI releases files on columnist Jack Anderson, NBC News (Oct. 11, 2008)..... 17

Government Surveillance: U.S. Has Long History of Watching White House Critics and Journalists, Newsweek (Jun. 23, 1975; republished Jul. 24, 2017) 17

II May's Constitutional History of England, 246 (Am. Ed. 1864) 13

James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times (Dec. 16, 2005) 19

Lana Sweeten-Shults, *Anonymous sources vital to journalism*, USA Today (Feb. 27, 2017) 20

Lindy Royce-Bartlett, *Leak Probe Has Chilled Sources, AP Exec Says*, CNN (Jun. 19, 2013)..... 21

Mark Sherman, *Gov't Obtains Wide AP Phone Records in Probe*, Associated Press (May 13, 2013) 21

Meeting in Person Most Common Way to Protect Sources, Pew Research Center (Feb. 4, 2015) 18

Michael Farrell, *Anonymous Sources*, SPJ Ethics Committee Position Paper..... 19

Scott Shane, David Johnston, James Risen, *Secret U.S. Endorsement of Severe Interrogations*, N.Y. Times (Oct. 4, 2007)..... 19

Souad Mekhennet and Joby Warrick, *U.S. Increasingly Sees Iran's Hand in the Arming of Bahraini Militants*, Wash. Post (Apr. 1, 2017) 19

Spencer S. Hsu, *Court: Warrantless requests to track cellphones, Internet use grew sevenfold in D.C. in three years*, Wash. Post (Jul. 18, 2017)..... 20

With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy, Human Rights Watch (Jul. 28, 2014) 21

INTEREST OF *AMICI CURIAE*[1]

The Reporters Committee for Freedom of the Press is an unincorporated nonprofit association of reporters and editors dedicated to safeguarding the First Amendment rights and freedom of information interests of the news media. Since 1970, the Reporters Committee has represented the interests of the press and the public in cases involving significant freedom of expression issues, including in this Court.

With some 500 members, American Society of News Editors ("ASNE") is an organization that includes directing editors of daily newspapers throughout the Americas. ASNE changed its name in April 2009 to American Society of News Editors and approved broadening its membership to editors of online news providers and academic leaders. Founded in 1922 as American Society of Newspaper Editors, ASNE is active in a number of areas of interest to top editors with priorities on improving freedom of information, diversity, readership and the credibility of newspapers.

The Associated Press Media Editors is a nonprofit, tax-exempt organization of newsroom leaders and journalism educators that works closely with The Associated Press to promote journalism excellence.

---

[1] Pursuant to Sup. Ct. R. 37, counsel for *amici curiae* state that no party's counsel authored this brief in whole or in part; no party or party's counsel made a monetary contribution intended to fund the preparation or submission of this brief; no person other than the *amici curiae*, its members or its counsel made a monetary contribution intended to fund the preparation or submission of this brief; and written consent of all parties to the filing of the brief has been filed with the Clerk of the Court.

APME advances the principles and practices of responsible journalism; supports and mentors a diverse network of current and emerging newsroom leaders; and champions the First Amendment and promotes freedom of information.

Association of Alternative Newsmedia ("AAN") is a not-for-profit trade association for 130 alternative newspapers in North America, including weekly papers like The Village Voice and Washington City Paper. AAN newspapers and their websites provide an editorial alternative to the mainstream press. AAN members have a total weekly circulation of seven million and a reach of over 25 million readers.

First Amendment Coalition is a nonprofit public interest organization dedicated to defending free speech, free press and open government rights in order to make government, at all levels, more accountable to the people. The Coalition's mission assumes that government transparency and an informed electorate are essential to a self-governing democracy. To that end, we resist excessive government secrecy (while recognizing the need to protect legitimate state secrets) and censorship of all kinds.

First Look Media Works, Inc. is a new non-profit digital media venture that produces The Intercept, a digital magazine focused on national security reporting.

Freedom of the Press Foundation is a non-profit organization that supports and defends public-interest journalism focused on transparency and accountability. The organization works to preserve and strengthen First and Fourth Amendment rights

guaranteed to the press through a variety of avenues, including public advocacy, legal advocacy, the promotion of digital security tools, and crowdfunding.

The International Documentary Association (IDA) is dedicated to building and serving the needs of a thriving documentary culture. Through its programs, the IDA provides resources, creates community, and defends rights and freedoms for documentary artists, activists, and journalists.

The Investigative Reporting Workshop, a project of the School of Communication (SOC) at American University, is a nonprofit, professional newsroom. The Workshop publishes in-depth stories at investigativereportingworkshop.org about government and corporate accountability, ranging widely from the environment and health to national security and the economy.

The Media Consortium is a network of the country's leading, progressive, independent media outlets. Our mission is to amplify independent media's voice, increase our collective clout, leverage our current audience and reach new ones.

MPA – The Association of Magazine Media, ("MPA") is the largest industry association for magazine publishers. The MPA, established in 1919, represents over 175 domestic magazine media companies with more than 900 magazine titles. The MPA represents the interests of weekly, monthly and quarterly publications that produce titles on topics that cover politics, religion, sports, industry, and virtually every other interest, avocation or pastime en-

joyed by Americans. The MPA has a long history of advocating on First Amendment issues.

The National Press Photographers Association ("NPPA") is a 501(c)(6) non-profit organization dedicated to the advancement of visual journalism in its creation, editing and distribution. NPPA's approximately 7,000 members include television and still photographers, editors, students and representatives of businesses that serve the visual journalism industry. Since its founding in 1946, the NPPA has vigorously promoted the constitutional rights of journalists as well as freedom of the press in all its forms, especially as it relates to visual journalism. The submission of this brief was duly authorized by Mickey H. Osterreicher, its General Counsel.

New England First Amendment Coalition is a non-profit organization working in the six New England states to defend, promote and expand public access to government and the work it does. The coalition is a broad-based organization of people who believe in the power of transparency in a democratic society. Its members include lawyers, journalists, historians and academicians, as well as private citizens and organizations whose core beliefs include the principles of the First Amendment. The coalition aspires to advance and protect the five freedoms of the First Amendment, and the principle of the public's right to know in our region. In collaboration with other like-minded advocacy organizations, NEFAC also seeks to advance understanding of the First Amendment across the nation and freedom of speech and press issues around the world.

The News Media Alliance is a nonprofit organization representing the interests of online, mobile and print news publishers in the United States and Canada. Alliance members account for nearly 90% of the daily newspaper circulation in the United States, as well as a wide range of online, mobile and non-daily print publications. The Alliance focuses on the major issues that affect today's news publishing industry, including protecting the ability of a free and independent media to provide the public with news and information on matters of public concern.

The News Guild – CWA is a labor organization representing more than 30,000 employees of newspapers, newsmagazines, news services and related media enterprises. Guild representation comprises, in the main, the advertising, business, circulation, editorial, maintenance and related departments of these media outlets. The News Guild is a sector of the Communications Workers of America. CWA is America's largest communications and media union, representing over 700,000 men and women in both private and public sectors.

Online News Association ("ONA") is the world's largest association of online journalists. ONA's mission is to inspire innovation and excellence among journalists to better serve the public. ONA's more than 2,000 members include news writers, producers, designers, editors, bloggers, technologists, photographers, academics, students and others who produce news for the Internet or other digital delivery systems. ONA hosts the annual Online News Association conference and administers the Online Journalism Awards. ONA is dedicated to advancing the interests of digital journalists and the public

generally by encouraging editorial integrity and independence, journalistic excellence and freedom of expression and access.

Radio Television Digital News Association ("RTDNA") is the world's largest and only professional organization devoted exclusively to electronic journalism. RTDNA is made up of news directors, news associates, educators and students in radio, television, cable and electronic media in more than 30 countries. RTDNA is committed to encouraging excellence in the electronic journalism industry and upholding First Amendment freedoms.

Reporters Without Borders has been fighting censorship and supporting and protecting journalists since 1985. Activities are carried out on five continents through its network of over 150 correspondents, its national sections, and its close collaboration with local and regional press freedom groups. Reporters Without Borders currently has 10 offices and sections worldwide.

Society of Professional Journalists ("SPJ") is dedicated to improving and protecting journalism. It is the nation's largest and most broad-based journalism organization, dedicated to encouraging the free practice of journalism and stimulating high standards of ethical behavior. Founded in 1909 as Sigma Delta Chi, SPJ promotes the free flow of information vital to a well-informed citizenry, works to inspire and educate the next generation of journalists and protects First Amendment guarantees of freedom of speech and press.

The Tully Center for Free Speech began in Fall, 2006, at Syracuse University's S.I. Newhouse School of Public Communications, one of the nation's premier schools of mass communications.

A journalist on assignment today is the proverbial one-man band with a cell phone for an instrument. Today, reporters use cell phones to set up and record interviews, write notes and articles, take pictures and video, share their work on social media, follow breaking news, research story tips, and engage in other functions essential to newsgathering. The cell phone has become a mobile newsroom. The government's ability, therefore, to reconstruct journalists' movements and location over an extended period of time using historical cell phone records threatens reporters' ability to maintain the confidentiality of their sources and gather the news. Because the government may seek a journalist's records in the course of a criminal investigation of another individual, such as a source, this threat exists even though a journalist's routine newsgathering is of course not a crime. Accordingly, this case presents a question critical to the news media: Whether the Fourth Amendment permits the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over an extended period of more than 125 days.

As news media organizations and organizations dedicated to protecting the First Amendment interests of journalists, amici have an interest in ensuring that the Fourth Amendment's protections against unreasonable searches and seizures are fully and strictly applied when the government seeks to obtain historical cell phone records showing a user's loca-

tion. Such records implicate First Amendment activities, including newsgathering, which will be chilled if warrantless acquisition of such records is routinely permitted. Properly applied, however, the Fourth Amendment affords protection to the exercise of First Amendment rights.

SUMMARY OF ARGUMENT

This case concerns the constitutionality of the warrantless acquisition by law enforcement of historical cellular telephone data revealing a comprehensive picture of an individual's location and movements. In this case, the government sought the data of a criminal suspect; but the standard governing such data adopted by the U.S. Court of Appeals for the Sixth Circuit below and advanced by the government here applies equally to the data of any cell phone user, including journalists. Because the Fourth Amendment's prohibition against "unreasonable searches and seizures" plays a vital role in protecting First Amendment rights, the question presented is one of particular importance to journalists and news organizations. Absent meaningful Fourth Amendment protection for records like those at issue in this case, activities protected by the First Amendment—including newsgathering, speech, expression, and association—will be chilled.

The Fourth Amendment's protection against unreasonable search and seizure is historically linked to the First Amendment's protection of the free press. As this Court has long recognized, the Fourth Amendment was ratified in response to the prerevolutionary practice of arresting publishers and confiscating papers to stifle dissenting viewpoints. The press's and the public's right to expressive and associational freedom therefore informs the scope of the Fourth Amendment's protection.

The records at issue in this case implicate precisely those rights. Historical cell site location information ("CSLI")—data gleaned from cell towers that

creates a record of an individual's location over time—can provide an intimate picture of an individual's political, professional, and religious associations. Such information can also reveal details about the newsgathering process, including reporters' communications with their sources, because the practical realities of contemporary newsgathering require journalists to carry and use cell phones on a near-constant basis. Due to the revelatory nature of location information, CSLI can be invasive even when it follows movements over a much shorter period of time than the 127-day tracking at issue in this case. The government's ability to acquire CSLI without meeting the Fourth Amendment's probable cause standard allows law enforcement to easily and routinely surveil both sources' and journalists' expressive, associational, and newsgathering activities, chilling individuals' willingness to engage in such activities.

In accord with the historical link between the First and Fourth Amendments, this Court has instructed lower courts to apply the Fourth Amendment with rigor when a search or seizure might implicate First Amendment interests. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978). Because CSLI reveals an individual's First Amendment-protected activities, it falls within the core category of information that the Fourth Amendment was designed to protect from warrantless surveillance. The U.S. Court of Appeals for the Sixth Circuit, below, however, expansively and erroneously applied the third-party doctrine to deprive the CSLI records at issue in this case of any Fourth Amendment protection. This ruling affects not just the rights of crimi-

nal suspects, but also the rights of any individual whose records could be relevant to any criminal investigation, which may include journalists.

For these reasons, *amici* urge this Court to reverse and to hold that the acquisition of CSLI records must satisfy the Fourth Amendment's requirements.

ARGUMENT

I. The history of the Fourth Amendment is intertwined with the First Amendment's guarantees of free expression and a free press.

The Fourth Amendment's prohibition against unreasonable searches and seizures arose from a long list of abusive English practices targeting printers and publishers of dissenting papers in the colonial era. Indeed, as this Court has stated, the history of the Fourth Amendment is "largely a history of conflict between the Crown and the press." *Stanford v. Texas*, 379 U.S. 476, 482 (1965). Pre-revolution "general warrants" allowed law enforcement to search "private houses for the discovery and seizure of books and papers that might be used to convict their owner of the charge of libel," to the detriment of the free press. *Boyd v. United States*, 116 U.S. 616, 626 (1886).

Two landmark cases that help to form the basis for our understanding of the Fourth Amendment's history and purpose—*Entick v. Carrington*, 19 How. St. Tr. 1029 (C.P. 1765), and *Wilkes v. Wood*, 19 How. St. Tr. 1153 (C.P. 1763)—involved the press. *See Marcus v. Search Warrant*, 367 U.S. 717, 724 (1961)

(explaining that these cases were "part of the intellectual matrix within which our own constitutional fabric was shaped").

In *Entick*, the British Secretary of State issued a general warrant for the arrest of a writer for a dissenting publication for seditious libel and the seizure of all of his papers. *See Stanford*, 379 U.S. at 483. The King's messengers ransacked the writer's house for four hours, seeking seditious material. *Id.* at 483–84. In an opinion this Court called "a wellspring of the rights now protected by the Fourth Amendment," Lord Camden declared the warrant unlawful: "His house is rifled, his most valuable secrets are taken out of his possession, before the paper for which he is charged is found to be criminal by any competent jurisdiction, and before he is convicted either of writing, publishing, or being concerned in the paper." *Id.* at 484 (quoting *Entick*, 19 How. St. Tr. At 1064). In response to *Entick*, the House of Commons passed two resolutions condemning such general warrants. *Id.* This Court has described *Entick* "as a 'monument of English freedom' 'undoubtedly familiar' to 'every American statesman' at the time the Constitution was adopted, and considered to be 'the true and ultimate expression of constitutional law'" in the area of search and seizure. *Brower v. County of Inyo*, 489 U.S. 593, 596 (1989) (quoting *Boyd*, 116 U.S. at 626).

A few years earlier in *Wilkes*, the Crown had similarly attempted to silence a publication that was anonymously published by John Wilkes, then a member of Parliament. *Stanford*, 379 U.S. at 483. The warrant in that case authorized the King's messengers "'to make strict and diligent search for the

authors, printers, and publishers of a seditious and treasonable paper, . . . and them, or any of them, having found, to apprehend and seize, together with their papers.'" *Id.* (quoting II May's Constitutional History of England, 246 (Am. Ed. 1864)). The messengers "set forth in quest of unknown offenders; and unable to take evidence, listened to rumors, idle tales, [ ] curious guesses," and "held in their hands the liberty of every man whom they were pleased to suspect." *Id.* at 483 (quoting II May's Constitutional History of England, 246 (Am. Ed. 1864)). Wilkes successfully sued the Secretary of State for damages, and Lord Camden condemned the general warrant, concluding that the "discretionary power given to messengers to search wherever their suspicions may chance to fall" was "totally subversive of the liberty of the subject." *Marcus*, 367 U.S. at 728–29 (quoting *Wilkes*, 19 How. St. Tr. at 1167).

Both *Entick* and *Wilkes* illustrate that "[t]he Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression," *Marcus*, 367 U.S. at 729, and for undermining the freedom of the press. When Congress drafted the Bill of Rights, Lord Camden's monumental *Entick* opinion was doubtlessly "in the minds of those who framed the [F]ourth [A]mendment." *Boyd*, 116 U.S. at 626–27; *see also Zurcher*, 436 U.S. at 569 (Powell, J., concurring) (noting that "[t]he Framers were painfully aware" of the history of conflict between the Crown and the press). As Justice Douglas put it, the First and Fourth Amendments "are indeed closely related, safeguarding not only privacy and protection against self-incrimination but 'conscience

and human dignity and freedom of expression as well.'" *Frank v. Maryland*, 359 U.S. 360, 376 (1959) (Douglas, J., dissenting) (internal citations omitted). Thus, concerns about free expression, and in particular about protections for an unfettered press, are at the core of the history of the Fourth Amendment. "It was in the setting of freedom of expression that Lord Camden denounced the general warrants," and the Fourth Amendment therefore must be understood as a response to the "'effort to destroy the freedom of the press.'" *Id.* (citation omitted). Because of the shared historical concerns of the First and Fourth Amendments, the modern-day experiences of the press are particularly relevant to understanding Fourth Amendment safeguards.

II. Warrantless acquisition of CSLI records chills the exercise of First Amendment rights, including newsgathering.

More than 200 years later, the application of the Fourth Amendment is complicated by the advent of new communications technologies, some of which are essential to free expression and the newsgathering process. Due to the ubiquitous nature of cell phones, location information gleaned from cell towers can disclose an individual's expressive and associational activities, as well as details about a journalist's newsgathering process. Such disclosure threatens to chill First Amendment-protected activities.

A. Long-term tracking of historical CSLI can reveal sensitive First Amendment-protected activities.

Communications technology is crucial to the exercise of free expression and association. Cell phones in particular have become "so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010). Thus, as cell phones become more sophisticated, and cellular phone and data providers gather more sensitive information about users, the risk that warrantless surveillance of individuals' locations will chill associational and expressive freedoms only increases.

The location-tracking capabilities of cell phones implicate unique First Amendment concerns. Over time, changes in technology have made CSLI information increasingly precise. These changes have included "smaller and smaller [cell sites] . . . which cover a very specific area, such as one floor of a building, the waiting room of an office, or a single home," and "the advent of smartphone 'pinging,' whereby location data can be generated almost continuously . . ." *United States v. Graham*, 824 F.3d 421, 448 (4th Cir. 2016) (citations omitted). Thus, like GPS data, CSLI is "qualitatively different" from physical records because it "can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Riley v. California*, 134 S. Ct. 2473, 2490 (2014). As the U.S. Court of Appeals for the D.C. Circuit stated when it considered the constitutionality of warrantless GPS monitoring, "A person who

knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts." *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd in part sub nom. United States v. Jones*, 565 U.S. 400 (2012); *see also State v. Earls*, 70 A.3d 630, 632 (N.J. 2013) (New Jersey Supreme Court noting that cell phones can reveal "not only where individuals are located at a point in time but also which shops, doctors, religious services, and political events they go to, and with whom they choose to associate"). Location data can therefore reveal extensive sensitive information about political, religious, and professional relationships. *See Jones*, 556 U.S. at 415 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").

Amici agree with Petitioner that *Riley* and *Jones* support the conclusion that CSLI can reveal a wealth of uniquely sensitive information. *See* Pet'r. Br. at 12, 38. The disclosure of such closely-held information may result in First Amendment harms. *See NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958) ("Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."). "Awareness that the Government may be watching chills associational and expressive freedoms." *Jones*, 565

U.S. at 416 (Sotomayor, J., concurring). Where surveillance implicates private location information, it can stifle dissent and the exercise of First Amendment rights. *See Government Surveillance: U.S. Has Long History of Watching White House Critics and Journalists*, Newsweek (Jun. 23, 1975; republished Jul. 24, 2017) (stating that in 1969 CIA agents "took photographs of White House demonstration leaders, recorded their auto license plates and sometimes even followed them home," and that the "CIA also followed newsmen in 1967, 1971 and 1972 in order to identify their sources"), https://perma.cc/B76N-3Z6B; *FBI releases files on columnist Jack Anderson*, NBC News (Oct. 11, 2008) (explaining that government documents obtained under the Freedom of Information Act reflected "summaries of [a columnist's] movements while under surveillance, and FBI memos detailing efforts to find his sources who leaked information from deep inside government agencies"), https://perma.cc/XD9R-FVM2.

First Amendment freedoms are protected not only from "frontal attack," but also from "being stifled by more subtle governmental interference." *Bates v. Little Rock*, 361 U.S. 516, 523 (1960). Warrantless acquisition of CSLI is the type of "subtle governmental interference" that can chill the robust exercise of associational and expressive rights.

B. CSLI acquisition threatens the news-gathering process.

CSLI can disclose particularly sensitive details about the journalistic process: It can reveal the stories a journalist is working on before they are published, where a journalist went to gather information

for those stories, and the identity of a journalist's sources. In part because location information can reveal so much about the journalistic process, reporters seek to ensure the locations where they meet their sources are kept private. Exposure of sources and journalistic methods can put sources' jobs and lives at risk, compromise the integrity of the newsgathering process, and have a chilling effect on reporting.

Among journalists, meeting in person with sources is widely considered the most secure form of communication. *See Meeting in Person Most Common Way to Protect Sources*, Pew Research Center (Feb. 4, 2015) (noting that 59% of reporters surveyed had met in person to protect a source), https://perma.cc/84RN-FRZ9. Confidentiality is a critical component of the reporter-source relationship, and effective newsgathering depends on an expectation of privacy in the location, time, and duration of those confidential meetings and communications. Communicating with confidential sources is a core journalistic practice and a necessary feature of investigative journalism. The confidentiality of these in-person meetings is compromised when law enforcement can obtain information about journalists' or sources' whereabouts without a warrant.

Some of the most important reporting on the functioning of government has depended on confidential sources. One of the most famous confidential sources, "Deep Throat," provided information to *Washington Post* reporters Bob Woodward and Carl Bernstein, exposing the Watergate scandal. More recently, news organizations have used confidential sources to report on harsh interrogations techniques

conducted by U.S. law enforcement, *see, e.g.*, Scott Shane, David Johnston, James Risen, *Secret U.S. Endorsement of Severe Interrogations*, N.Y. Times (Oct. 4, 2007), http://nyti.ms/1dkyMgF; the Central Intelligence Agency's use of a network of secret prisons for terrorism suspects, *see, e.g.*, Dana Priest, *CIA Holds Terror Suspects in Secret Prisons*, Wash. Post (Nov. 2, 2005), http://wapo.st/Ud8UD; and an illegal wiretapping program at the National Security Agency, *see, e.g.*, James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times (Dec. 16, 2005), http://nyti.ms/nelMIB. In the last year, reporters have relied upon confidential sources to inform the public about everything from foreign policy, *see, e.g.*, Souad Mekhennet and Joby Warrick, *U.S. Increasingly Sees Iran's Hand in the Arming of Bahraini Militants*, Wash. Post (Apr. 1, 2017), https://perma.cc/ZUA4-8HV7, to foreign threats to the 2016 presidential election, *see, e.g.*, Eric Lichtblau, *C.I.A. Tracked Russian Prying in the Summer*, N.Y. Times (Apr. 7, 2017), https://nyti.ms/2oOwTBz.

As these examples demonstrate, investigative reporting based on confidential sources is a necessary part of the fabric of an informed democratic society and fosters the civic literacy that forms the bedrock of democratic discourse. According to the Society of Professional Journalists, although identifying sources is ideal, "[a]nonymous sources are sometimes the only key to unlocking that big story, throwing back the curtain on corruption, fulfilling that journalistic missions of watchdog on the government and informant to the citizens." Michael Farrell, *Anonymous Sources*, SPJ Ethics Committee Position Paper,

https://perma.cc/5BQB-SRA3. Indeed, without confidential sources, journalists "would be relying on the official side of the story, and the official side of a story isn't always the whole side." Lana Sweeten-Shults, *Anonymous sources vital to journalism*, USA Today (Feb. 27, 2017), https://perma.cc/AV7V-Z4K8.

Although confidentiality is of utmost importance, contemporary investigative newsgathering often depends on a smartphone. Cell phones now serve as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers"—all tools that are integral to the journalistic profession. *Riley*, 134 S. Ct. at 2489. Journalists use cell phones to email sources and editors, write pitches, record interviews, capture photos and video to accompany stories, conduct research, monitor breaking news, and engage with their readership on platforms such as Twitter and Facebook. Leaving a cell phone behind while conducting field research and meeting with sources on a regular basis would severely hamper the goal of gathering details about a story.

Journalists are aware that the government is increasingly using electronic surveillance in general—and specifically the Stored Communications Act ("SCA"), 18 U.S.C. § 2703(d), orders at issue in this case—to target cell phones and similar communication devices. *See* Spencer S. Hsu, *Court: Warrantless requests to track cellphones, Internet use grew sevenfold in D.C. in three years*, Wash. Post (Jul. 18, 2017), https://perma.cc/W6TN-VVGW (explaining that warrantless SCA requests to the U.S. District Court for the District of Columbia grew sevenfold in the past three years). Concerns about the vast scope of sur-

veillance has already caused some journalists to take steps to try to avoid that surveillance—including limiting their use of important tools that are critical to newsgathering. *See With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy*, Human Rights Watch (Jul. 28, 2014), https://perma.cc/LJ9E-88YS (noting in a 120-page study that several journalists reported turning off their phones, removing phone batteries, or leaving phones behind when meeting in person with sources); *see also* Dan Gillmore, *Beyond Encryption*, Colum. J. Rev. (May 7, 2012), https://perma.cc/43DN-SNPN ("If you do need to talk to [a source] using a cell phone, Fed-Ex them a prepaid phone, and tell them not to use it, or even turn it on, near their home/office.").

Surveillance has also made sources less willing to inform reporters about issues of public concern. In 2013, for example, the Associated Press learned that the Justice Department had seized records from twenty AP telephone lines used by more than 100 AP reporters and editors. *See* Mark Sherman, *Gov't Obtains Wide AP Phone Records in Probe*, Associated Press (May 13, 2013), https://perma.cc/2P8J-RTPT. AP President and CEO Gary Pruitt discussed the impact of the surveillance during a speech at the National Press Club: "In some cases, government employees that we once checked in with regularly will no longer speak to us by phone and some are reluctant to meet in person." Lindy Royce-Bartlett, *Leak Probe Has Chilled Sources, AP Exec Says*, CNN (Jun. 19, 2013), https://perma.cc/VU8T-6HUP.

As Justice Marshall wrote nearly forty years ago in his dissenting opinion in *Smith v. Maryland*,

"Permitting governmental access to telephone records on less than probable cause may [ ] impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society." 442 U.S. 735, 751 (1979) (Marshall, J., dissenting). It is unsurprising that fear of warrantless location tracking chills reporter-source communications and impedes newsgathering, harming the flow of information to the public.

III. Fourth Amendment protections should be rigorously applied when the government seeks to obtain CSLI because First Amendment interests are at stake.

Amici agree with Petitioner that the Fourth Amendment should apply when the government seeks to obtain CSLI. In addition to the reasons set forth by Petitioner, Fourth Amendment protections should also apply because CSLI implicates First Amendment rights.

Consistent with the historic relationship between the First and Fourth Amendments, *see supra* Section I, this Court has found that where the materials to be searched "may be protected by the First Amendment, the requirements of the Fourth Amendment must be applied with 'scrupulous exactitude.'" *Zurcher*, 436 U.S. at 564 (quoting *Stanford*, 379 U.S. at 485). In *Zurcher*, this Court considered the constitutionality of a search warrant authorizing the search of a newspaper's office for evidence of a crime. *Id.* at 563. The Court held that, under the particular facts of that case, the Fourth Amendment's warrant requirements were sufficiently protective of First Amendment rights. *Id.* Specifically, this Court stat-

ed that "[p]roperly administered, the preconditions for a warrant—probable cause, specificity with respect to the place to be searched and the things to be seized, and overall reasonableness—should afford sufficient protection against the harms that are assertedly threatened by warrants for searching newspaper offices." *Id.* at 565. These Fourth Amendment safeguards are the minimum necessary for protecting against First Amendment harms.

The form of process at issue in this case—an order under the Stored Communications Act—lacks any Fourth Amendment safeguards at all. SCA orders for historical CSLI do not require probable cause, reasonableness, or specificity with respect to the scope of the search. Rather, they require only a showing of "specific and articulable facts" demonstrating that the material sought is "relevant and material" to an investigation. 18 U.S.C. § 2703(d). This lower standard impermissibly permits the government to obtain CSLI, which implicates associational, expressive, and newsgathering activities, without satisfying the Fourth Amendment safeguards found in *Zurcher* to be sufficient to protect First Amendment rights

IV. The U.S. Court of Appeals for the Sixth Circuit's application of the third-party doctrine to CSLI records imperils the free and unfettered exercise of First Amendment rights.

The U.S. Court of Appeals for the Sixth Circuit, below, held that the government's collection of Petitioner's CSLI was not a Fourth Amendment-protected search because Petitioner had no reasona-

ble expectation of privacy in CSLI created and maintained by a cellular service provider. *United States v. Carpenter*, 819 F.3d 880, 889–90 (6th Cir. 2016). In reaching this holding, the divided three-judge panel relied upon this Court's decisions in *Smith*, 442 U.S. 735, and *United States v. Miller*, 425 U.S. 435 (1976). *Id.* at 887–89; *see also United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (en banc), *cert. denied*, 136 S. Ct. 479 (2015), (similarly holding that *Smith* and *Miller* lead to the conclusion that there is no Fourth Amendment protection for CSLI records); *Graham*, 824 F.3d 421 (same); *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013) (same). *Compare In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010) (distinguishing *Smith* and holding that a magistrate judge has the discretion to require a warrant for CSLI). Contrary to this Court's instruction that Fourth Amendment requirements be applied with "scrupulous exactitude" when law enforcement seeks to obtain material that "may be protected by the First Amendment," *Zurcher*, 436 U.S. at 564, the panel's decision interpreted the so-called third-party doctrine so broadly as to seemingly foreclose *any* application of the Fourth Amendment's protections to CSLI.

In *Miller*, this Court held that a bank customer has no reasonable expectation of privacy in checks and deposit slips held by a bank because that information was voluntarily "revealed to a third party"—*i.e.*, the bank. *See Miller*, 425 U.S. at 442. In *Smith* the Court applied similar reasoning in the context of a telephone company, finding no "legitimate expecta-

tion of privacy in the numbers [petitioner] dialed" over a short period of time, which the government obtained from the phone company using a subpoena. 442 U.S. at 742.

Lower courts have drawn from these cases the proposition that individuals do not have a Fourth Amendment protected interest in information voluntarily conveyed to third parties—what has come to be known in Fourth Amendment jurisprudence as the third-party doctrine. *See Graham*, 824 F.3d at 425 (citing *Smith* and *Miller* to explain the "rule—the third-party doctrine," which states "that an individual enjoys no Fourth Amendment protection 'in information he voluntarily turns over to [a] third part[y]" (internal citations omitted)); *Davis*, 785 F.3d at 512. As this Court has recognized, however, a "mechanical interpretation" of the third-party doctrine, especially in the context of advancing technology, can erode constitutional rights. *Kyllo v. United States*, 533 U.S. 27, 35 (2001); *see also Davis*, 785 F.3d at 537 (Martin, J., dissenting) (describing the "slippery slope that would result from a wooden application of the third-party doctrine").

As explained above, First Amendment rights are placed in jeopardy when law enforcement can, broadly-speaking, invade the privacy of professional, political, and religious associations without a warrant. *See supra* Section II. And an overbroad application of the third-party doctrine is particularly pernicious to the press. Although the third-party doctrine is based on the premise that parties voluntarily convey information to third-party companies, journalists, like other cell phone users, do not "voluntarily" share their location with a cell phone provider "in any

meaningful way," *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 317, because there is no action in placing or receiving a call that would alert the journalist that he or she is conveying location information to the wireless carrier. Although journalists are aware of location tracking, they and their sources may be unaware of the extent and specifics of the surveillance—namely, that cell service providers obtain and store CSLI. *See id.* ("[I]t is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information.").

Even if journalists are aware that service providers collect historical CSLI, journalists are dependent on their cell phones to contact sources, communicate with editors, disseminate news, and generally engage in the craft of contemporary newsgathering. *See Graham*, 825 F.3d at 445–46 (Wynn, J., dissenting in part and concurring in the judgment) (finding that CSLI is not voluntarily conveyed by a cell phone user in part because "CSLI is purely a function and product of cellular telephone technology, created by the provider's system network . . .") (quoting *Commonwealth v. Augustine*, 4 N.E.3d 846, 862 (2014)). Because third-party cell service companies obtain users' location data "for the specific purpose of directing the routing of information," *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008), journalists necessarily must allow cell service companies to obtain their CSLI in order to use a cell phone. As Justice Sotomayor noted in *Jones*, the third-party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about them-

selves to third parties in the course of carrying out mundane tasks." 565 U.S. at 417 (Sotomayor, J., concurring). Journalists in particular reveal a great deal of information when using cell phones, not only in the course of carrying out routine tasks, but also in the course of gathering and disseminating the news.

As this Court previously recognized, magistrate judges assessing warrant applications play a crucial role in assuring that "the requirements of specificity and reasonableness are properly applied, policed, and observed" to protect First Amendment rights, including those of journalists. *Zurcher*, 436 U.S. at 566. When the third-party doctrine is expanded to permit warrantless acquisition of location data, that vital check on government overreach that is essential to enabling the full-throated exercise of First Amendment rights disappears. A Fourth Amendment warrant, and nothing less, is necessary to protect the interests of the press and public in the context of long-term CSLI tracking. "No less a standard could be faithful to First Amendment freedoms." *Stanford*, 379 U.S. at 485.

CONCLUSION

For the foregoing reasons, *amici* respectfully urge this Court to reverse the U.S. Court of Appeals for the Sixth Circuit opinion below.

Respectfully submitted,

Bruce D. Brown
Counsel of Record
Caitlin Vogus
Selina MacLaren
THE REPORTERS COMMITTEE
FOR FREEDOM OF THE PRESS
1156 15th St. NW, Suite 1250
Washington, DC 20005
bbrown@rcfp.org
(202) 795-9300

*Additional counsel for *amici* are listed in Appendix A.

August 14, 2017

APPENDIX A

Additional counsel for *Amici Curiae*

Kevin M. Goldberg
Fletcher, Heald & Hildreth, PLC
1300 N. 17th St., 11th Floor
Arlington, VA 22209
Counsel for American Society of News Editors
Counsel for Association of Alternative Newsmedia

David Snyder
First Amendment Coalition
534 Fourth St., Suite B
San Rafael, CA 94901

James Cregan
Executive Vice President
MPA – The Association of Magazine Media
1211 Connecticut Ave. NW Suite 610
Washington, DC 20036

Mickey H. Osterreicher
1100 M&T Center, 3 Fountain Plaza,
Buffalo, NY 14203
Counsel for National Press Photographers Association

Robert A. Bertsche (BBO #554333)
Prince Lobel Tye LLP
100 Cambridge Street
Boston, MA 02114
Counsel for the New England First Amendment Coalition

Kurt Wimmer
Covington & Burling LLP
850 10th Street NW
Washington, DC 20001
Counsel for the News Media Alliance

Barbara L. Camens
Barr & Camens
1025 Connecticut Ave., NW
Suite 712
Washington, DC 20036
Counsel for The Newspaper Guild - CWA

Laura R. Handman
Alison Schary
Davis Wright Tremaine LLP
1919 Pennsylvania Avenue, NW
Suite 800
Washington, DC 20006
Counsel for Online News Association

Thomas R. Burke
Davis Wright Tremaine LLP
Suite 800
500 Montgomery Street
San Francisco, CA 94111
Counsel for Online News Association

Kathleen A. Kirby
Wiley Rein LLP
1776 K St., NW
Washington, DC 20006
Counsel for Radio Television Digital News Association

Bruce W. Sanford
Mark I. Bailen
Baker & Hostetler LLP
1050 Connecticut Ave., NW
Suite 1100
Washington, DC 20036
Counsel for Society of Professional Journalists

RECORD AND BRIEFS

No. 16-402

Supreme Court, U.S.
FILED
AUG 14 2017
OFFICE OF THE CLERK

In The

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Sixth Circuit

BRIEF OF *AMICUS CURIAE* RESTORE THE FOURTH, INC. IN SUPPORT OF PETITIONER

MAHESHA P. SUBBARAMAN
Counsel of Record
SUBBARAMAN PLLC
222 S. 9th St., Ste. 1600
Minneapolis, MN 55402
(612) 315-9210
mps@subblaw.com

August 14, 2017

COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

Library of Congress

TABLE OF CONTENTS

Page

Table of Authorities ii

Interest of the *Amicus Curiae* 1

Summary of the Argument 2

Argument 3

I. The Court's Fourth Amendment analysis of cell-site location information (CSLI) should recognize that privacy is relational 3

II. The Court's Fourth Amendment analysis of CSLI should recognize that CSLI will become even more revealing over time 9

III. The Court's Fourth Amendment analysis of CSLI should recognize that police use of CSLI comes with a high risk of abuse 14

Conclusion 18

TABLE OF AUTHORITIES

Page

CASES

Boyd v. United States, 116 U.S. 616 (1886) 3, 10, 18

Brinegar v. United States, 338 U.S. 160 (1949) 15, 16

Cohens v. Virginia, 19 U.S. 264 (1821) 9

Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014) 10

Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 659 (D.N.J. 2013) 7

Elonis v. United States, 135 S. Ct. 2001 (2015) 7

Kyllo v. United States, 533 U.S. 27 (2001) 9, 10, 13

Lane v. Facebook, Inc., 696 F.3d 811 (9th Cir. 2012) 7, 8

Miller v. United States, 425 U.S. 435 (1976) 4

Olmstead v. United States, 277 U.S. 438 (1928) 2, 4, 5

Ornelas v. United States, 517 U.S. 690 (1996) 3

Riley v. California, 134 S. Ct. 2473 (2014) 19

Smith v. Maryland, 442 U.S. 735 (1979) 4

State v. Earls, 70 A.3d 630 (N.J. 2013) 11

State v. Tate, 849 N.W.2d 798 (Wis. 2014) 9

United States v. Carloss, 818 F.3d 988 (10th Cir. 2016) 6, 8

United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016) 10

TABLE OF AUTHORITIES – Continued

Page

United States v. Jones, 565 U.S. 400 (2012) 8

Weems v. United States, 217 U.S. 349 (1910) 9, 11

CONSTITUTIONAL PROVISION

U.S. Const., amend. IV .....*passim*

OTHER AUTHORITIES

AMNESTY INT'L, "IT'S ENOUGH FOR PEOPLE TO FEEL IT EXISTS": CIVIL SOCIETY, SECRECY, & SURVEILLANCE IN BELARUS (2016), http://bit.ly/2uuF7Fv 16, 17

Andrea Peterson, *LOVEINT: When NSA Officers Use Their Spying Power on Love Interests*, WASH. POST, Aug. 24, 2013, http://wapo.st/15kehuK 16

Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA TODAY, Aug. 23, 2015, http://usat.ly/1JeqgNk 15

Brian L. Owsley, *TriggerFish, StingRays, & Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183 (2014) 13

Charles Blain, *Police Could Get Your Location Data Without a Warrant. That Has to End*, WIRED, Feb. 2, 2017, http://bit.ly/2jGGRkA 16

Frank Main, *Chicago Cops Lose Bid to Toss Lawsuit Over Secret Cell-Phone Tracking*, CHICAGO SUN-TIMES, Jan. 11, 2016, http://bit.ly/2uwZc9M 17, 18

TABLE OF AUTHORITIES – Continued

Page

If These Walls Could Talk: The Smart Home & the Fourth Amendment Limits of the Third Party Doctrine, 130 HARV. L. REV. 1924 (2017) 14

Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205 (2015) 12

Jennifer Valentino-DeVries, *Police Snap Up Cheap Cellphone Trackers*, WALL ST. J., Aug. 19, 2015, http://on.wsj.com/2ux3Ep0 18

Jonathan Bard, *Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment*, 57 BOSTON COLLEGE L. REV. 731 (2016) 13

Laurent Sacharoff, *The Relational Nature of Privacy*, 16 LEWIS & CLARK L. REV. 1249 (2012) 4, 5

Mara H. Gottfried, *Minneapolis Officer Quits Amid Federal Probe of Metro Gang Strike Force*, PIONEER PRESS, Aug. 28, 2009, http://bit.ly/2vWk1is 16

Michael Byrne, *New Indoor Positioning System Tracks Your Phone Using Sound Waves*, MOTHERBOARD, Apr. 2, 2016, http://bit.ly/2fEm5Wd 12

Natasha H. Duarte, *The Home Out of Context: The Post-*Riley *Fourth Amendment & Law Enforcement Collection of Smart Meter Data*, 93 N.C. L. REV. 1140 (2015) 14

Parmy Olson, *Algorithm Aims to Predict Crime by Tracking Mobile Phones*, FORBES, Aug. 6, 2012, http://bit.ly/2wzXDcO 12

TABLE OF AUTHORITIES – Continued

Page

Robert H. Sloan & Richard Warner, *Relational Privacy: Surveillance, Common Knowledge, and Coordination*, 11 UNIV. OF ST. THOMAS J.L. & PUB. POL'Y 1 (2017).....6

Robert M. Bloom & William T. Clark, *Small Cells, Big Problems: The Increasing Precision of Cell Site Location Information & the Need for Fourth Amendment Protections*, 106 J. CRIM. LAW & CRIMINOLOGY 167 (2016).....11

Tom Simonite, *Bringing Cell-Phone Location-Sensing Indoors*, MIT TECH. REV., Aug. 31, 2010, http://bit.ly/2fEJcA9.....12

Tom Simonite, *This Phone App Knows If You're Depressed*, MIT TECH. REV., Sept. 22, 2014, http://bit.ly/2w35PoW.....12

WESLEY CHENG, CTR. FOR THE ADVANCEMENT OF PUBLIC INTEGRITY, COLUMBIA LAW SCHOOL, DOES SEEKING CELL SITE LOCATION INFORMATION REQUIRE A SEARCH WARRANT? (2016), http://bit.ly/2uuCOSB.....14

INTEREST OF THE *AMICUS CURIAE*[1]

Restore the Fourth, Inc. is a national, non-partisan civil liberties organization dedicated to robust enforcement of the Fourth Amendment to the United States Constitution. Restore the Fourth believes that everyone is entitled to privacy in their persons, homes, papers, and effects and that modern changes in technology, governance, and law should foster the protection of this right.

To advance these principles, Restore the Fourth oversees a network of local chapters, whose members include lawyers, academics, advocates, and ordinary citizens. Each chapter devises a variety of grassroots activities designed to bolster political recognition of Fourth Amendment rights. On the national level, Restore the Fourth also files amicus briefs in significant Fourth Amendment cases.[2]

---

[1] This amicus brief is filed based on the blanket letters of consent that both Petitioner and Respondent have filed with the Court. No counsel for a party authored this brief in whole or in part; nor has any person or entity, other than Restore the Fourth, Inc. and its counsel, contributed money intended to fund the preparation or submission of this brief.

[2] *See, e.g.*, Brief of *Amicus Curiae* Restore the Fourth, Inc. in Support of Petitioners, *Hernandez v. Mesa*, 137 S. Ct. 2003 (2017) (No. 15-118); Brief of *Amicus Curiae* Restore the Fourth, Inc. in Support of Plaintiff-Appellee Araceli Rodriguez, *Rodriguez v. Swartz*, No. 15-16410 (9th Cir. filed May 7, 2016); Brief of *Amicus Curiae* Restore the Fourth, Inc. in Support of Defendant-Appellant Stavros Ganias, *United States v. Ganias*, 824 F.3d 199 (2d. Cir. 2016) (No. 12-240-cr) (en banc).

SUMMARY OF THE ARGUMENT

Nearly 90 years ago, Justice Brandeis warned that the "progress of science in furnishing the Government with means of espionage [was] not likely to stop with wire-tapping." *Olmstead v. United States*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting). Justice Brandeis also predicted "[w]ays may some day be developed" that would let the government pry into a person's "unexpressed beliefs, thoughts, and emotions." *Id.*

That day has arrived.

This case is about cell-site location information, or CSLI, which is generated when a person uses a cell phone. CSLI currently makes it possible for the police to know every place that a person has been and every social connection that a person has made over a period of time. CSLI also stands to make it possible for the police to predict a person's future location with a high degree of accuracy. Hence, with a person's CSLI in hand, the police now have the power to pry into that person's unexpressed beliefs, thoughts, and emotions.

Given this reality, any Fourth Amendment analysis of CSLI should be guided by the following three principles. First, privacy is relational in nature, which means that persons may have a reasonable expectation of privacy in their disclosures to third parties (e.g., a wireless service provider). Second, technological innovation will render CSLI even more revealing over time. Third, practical experience teaches that police use of CSLI comes with high risk of abuse.

ARGUMENT

I. The Court's Fourth Amendment analysis of cell-site location information (CSLI) should recognize that privacy is relational.

The Fourth Amendment to the United States Constitution states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." This language "demonstrates a strong preference for searches [to be] conducted pursuant to a warrant." *Ornelas v. United States*, 517 U.S. 690, 699 (1996).

This preference cannot be enforced, however, without some explanation of the privacy interests that the Fourth Amendment is meant to protect. A definition of privacy is central to identifying whether a "search" has taken place and, if so, whether the warrant rule or an exception applies (e.g., exigent circumstances). This Court's early Fourth Amendment jurisprudence bears out this point. In *Boyd v. United States*, the Court emphasized that the Fourth Amendment is about more than "the breaking of . . . doors, and the rummaging of . . . drawers." 116 U.S. 616, 630 (1886). Rather, the Fourth Amendment is meant to address "all invasions on the part of the government and its employés of . . . the privacies of life." *Id.*

The Court's subsequent analysis of the privacies of life has led the Court to conclude that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). The Court has justified this conclusion on the ground that a person "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *Miller v. United States*, 425 U.S. 435, 443 (1976). And the Court has found this conclusion holds true even when a person reveals information to a third party "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.*

This analysis reduces the Fourth Amendment's protection of the privacies of life to "an all-or-nothing concept," such that once "a person has waived or ceded privacy to one person she has ceded it to all."[3] But that is not how privacy works in the real world, nor is it consistent with the intent of the Framers in adopting the Fourth Amendment. Justice Brandeis recognized as much in his now-celebrated dissent in *Olmstead v. United States*, 277 U.S. 438 (1928). Rejecting the majority's conclusion that the Fourth Amendment did not apply to police wiretapping, Justice Brandeis explained that by adopting the Fourth Amendment, the Framers "conferred, **as against the**

---

[3] Laurent Sacharoff, *The Relational Nature of Privacy*, 16 LEWIS & CLARK L. REV. 1249, 1251 (2012).

Government, the right to be let alone." *Id.* at 478 (bold added).

Justice Brandeis thus made it clear that privacy is *relational* in nature, and the Fourth Amendment is concerned with shielding the privacies of life *from the government*. That purpose cannot be advanced by the conclusion that no reasonable expectation of privacy can reside in what we choose to disclose to third parties *who are not the government*. "[C]ommon sense tells us we treat privacy differently with different people and different classes of people. What we disclose to a spouse or partner we might not wish to disclose to the public or even a friend."[4] By the same token, our willingness to disclose information to a friend or a third-party service provider does not translate to a willingness to disclose the same information to the government—an entity that is "certainly different from friends and . . . private institutions—its criminal enforcement arm so much the greater."[5]

The relational nature of privacy is also apparent from the reality that "[w]hen we talk about privacy we must look at the manner and purpose of any intrusion."[6] "If a doctor looks in someone's wallet to find an emergency contact, that is far less an intrusion than if

---

[4] *Id.* at 1271.

[5] *Id.* at 1274.

[6] *Id.* at 1250.

a jealous spouse looks there for evidence of infidelity . . . .[7] Likewise, "a [police] officer approaching your home to return your lost dog or to solicit for charity may not be conducting a 'search' within the meaning of the Fourth Amendment. But one calling to investigate a crime surely is." *United States v. Carloss*, 818 F.3d 988, 1004 (10th Cir. 2016) (Gorsuch, J., dissenting).

Finally, the relational nature of privacy is apparent from the social limits that third parties observe when information is disclosed to them. These "specific patterns of informational restraint" depend on "the social roles in which people interact."[8] For example, pharmacists tend not to view the disclosure of prescription information to them as license to ask about their customers' personal lives.[9] It therefore makes no sense to conclude that individuals can never have any reasonable expectation of privacy in their disclosures to third parties. Depending on the social relationship involved, the exact opposite is often true: disclosures to a third party are often the result of people reasonably expecting that a third party will neither pry into the disclosure nor exploit it (i.e., as distinct from the mere expectation that a third party will not reveal the disclosure to others).

---

[7] *Id.*

[8] Robert H. Sloan & Richard Warner, *Relational Privacy: Surveillance, Common Knowledge, and Coordination*, 11 UNIV. OF ST. THOMAS J.L. & PUB. POL'Y 1, 7 (2017).

[9] *See id.*

The digital age, in turn, makes understanding privacy in relational terms all the more important. Consider the "social networking Web site Facebook." *Elonis v. United States*, 135 S. Ct. 2001, 2004 (2015). Facebook enables users to "post items . . . that are accessible to other users" and to the general public. *Id.* Facebook also "allows users to select privacy settings" that limit the public visibility of user posts. *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 659, 668 (D.N.J. 2013). "Access can be limited to the user's Facebook friends, to particular groups or individuals, or to just the user." *Id.* This means that privacy on Facebook is not an all-or-nothing decision between global disclosure and total secrecy. Instead, privacy is a relational matter, with users choosing who gets to see their posts and who does not.

It is for this reason that a public revolt occurred in 2007 when Facebook adopted a new advertising program called Beacon. *See Lane v. Facebook, Inc.*, 696 F.3d 811, 816 (9th Cir. 2012). Through this program, the profiles of Facebook users began to display information about these users' activities on other websites—e.g., book purchases they made on a bookseller's website. *See id.* Facebook did not seek user consent for these disclosures. *See id.* As a result, many Facebook users "complained that Beacon was causing publication of otherwise private information about their outside web activities to their personal profiles without their knowledge or approval." *Id.* These complaints—and considerable public outcry—led Facebook to end Beacon and to pay $9.5 million to settle a class-action

lawsuit alleging Beacon violated various consumer privacy laws. *See id.* at 816–17.

While digital age developments like Facebook Beacon shed new light on the relational nature of privacy, they are not the only proof of this reality. Similar proof may be found in the "common-law trespassory test" for Fourth Amendment violations that this Court has revived in recent years. *United States v. Jones*, 565 U.S. 400, 414 (2012). The history behind this test teaches that the preservation of privacy through property rights is not an all-or-nothing proposition. One can license third parties to access one's private property while still retaining ultimate control over the property. *See Carloss*, 818 F.3d at 1006 (Gorsuch, J., dissenting) ("[T]he original meaning of the Fourth Amendment [and] centuries of common law recogniz[es] that homeowners may revoke by word or deed the licenses they themselves extend."). The quintessential example of this is a "no trespassing" sign, which lets property owners choose which third parties are welcome on their property (if any) and which ones are not. *See id.* at 1005 (explaining that homeowners may use no-trespassing signs to "mak[e] it clear to . . . 'solicitors, hawkers, and peddlers,' . . . that their presence on the curtilage is unwelcome").

With this in mind, the Court should commence its Fourth Amendment analysis of cell-site location information by "reconsider[ing] the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). The Fourth Amendment allows us to hold private *as*

against the government that which we share with others. And under this relational view of privacy, the Fourth Amendment status of CSLI may boil down to one simple fact: "People do not buy cell phones to have them serve as government tracking devices. They do not expect the government to track them by using [CSLI] . . . ." *State v. Tate*, 849 N.W.2d 798, 815 (Wis. 2014) (Abrahamson, C.J., dissenting).

II. The Court's Fourth Amendment analysis of CSLI should recognize that CSLI will become even more revealing over time.

In applying the Fourth Amendment, this Court has long recognized that it must contemplate not only "what has been" but also "what may be." *Weems v. United States*, 217 U.S. 349, 374 (1910). For good reason. "Time works changes" and "brings into existence new conditions and purposes." *Id.* Forward-looking Fourth Amendment analysis subsequently ensures that "[r]ights declared in words" are not "lost in reality." *Id.*; *see also Cohens v. Virginia*, 19 U.S. 264, 387 (1821) (Marshall, C.J.) ("[A] constitution is framed for ages to come, and is designed to approach immortality as nearly as human institutions can approach it.").

Forward-looking Fourth Amendment analysis is especially critical where new technology is involved. *Kyllo v. United States*, 533 U.S. 27 (2001) cements this point. Confronted with the warrantless use of a thermal imager to view the inside of a home, this Court recognized that it could not confine its Fourth Amendment analysis to the "relatively crude" imager at issue.

Id. at 36. The Court also had to consider the "more sophisticated systems that are already in use or in development." *Id.* This led the Court to find that a Fourth Amendment violation had occurred. *See id.* The Court thereby refused to "leave the homeowner at the mercy of advancing technology . . . that could discern all human activity in the home." *Id.*

Similar forward-looking concern is required in any Fourth Amendment analysis of cell-site location information. In this case, the CSLI at issue consists of the call records that a wireless cellular provider logged and stored over a 127-day period for a single cell-phone subscriber (Mr. Carpenter). *See United States v. Carpenter*, 819 F.3d 880, 885–86 (6th Cir. 2016). The call records established the "date, time, and length of each call" that the subscriber made during the 127-day period. *Id.* The call records also established "the phone numbers engaged on [each] call" and "the cell sites where the call began and ended." *Id.* And with these call records in hand, the police were able to create maps showing that the subscriber's phone was located within 0.5 to 2 miles of certain robbery sites around when each robbery occurred. *Id.*

From this bare description of the CSLI at issue in this case, it is already possible to discern the remarkable capacity of CSLI to intrude on "the privacies of life." *Boyd*, 116 U.S. at 630. Indeed, CSLI constitutes "a treasure trove of very detailed and extensive information about [an] individual's 'comings and goings' in both public and private places." *Commonwealth v. Augustine*, 4 N.E.3d 846, 863 (Mass. 2014). And this treasure trove includes "not only where individuals are located at a point in time but also which shops,

doctors, religious services, and political events they go to, and [the persons] with whom they choose to associate." *State v. Earls*, 70 A.3d 630, 632 (N.J. 2013).

But this is only the beginning for CSLI. Contemplating "what may be" in regard to CSLI points to a future in which CSLI reveals even more about the privacies of life. *Weems*, 217 U.S. at 374. This is true for at least three reasons:

First, "[b]ecause of recent evolutions in cellular network technology, CSLI will soon paint an even more precise picture of a person's location history."[10] In particular, the growing "integration of small cell technologies into cellular networks" will enable CSLI to "reveal a cell phone user's location to within fewer than ten feet."[11] CSLI will consequently become even "more accurate than location data generated from GPS technologies, which can determine location to within only fifty feet."[12] And this innovation stands to become a reality sooner rather than later given that the Federal Communications Commission has "recently updated its rules on cellular networks to promote the installation of small cells."[13]

---

[10] Robert M. Bloom & William T. Clark, *Small Cells, Big Problems: The Increasing Precision of Cell Site Location Information & the Need for Fourth Amendment Protections*, 106 J. CRIM. LAW & CRIMINOLOGY 167, 170 (2016).

[11] *Id.* at 176.

[12] *Id.*

[13] *Id.* Another way CSLI stands to paint a more detailed portrait of a person's location history is through the advent of new

Second, the power and capacity of computers to extract meaning from CSLI grows with each passing day. Computing in general "facilitates aggregation, persistence, and searchability."[14] Applied to CSLI, sophisticated computing algorithms may soon make it possible for CSLI to reveal not only where a given person has been but also where that person is likely to be in the future. In fact, one researcher has already accomplished this feat on a small scale, "predicting the movements of 25 volunteers working in a town in Switzerland."[15] "He used GPS data, telephone numbers and their texting and calling history to do it, and the algorithm was at times able to predict where these volunteers were heading to within 20 square meters."[16]

Third, the number of devices enabling the police to obtain CSLI without going through a third-party wireless provider continues to grow. These devices go

---

technologies that make it easier for cell phones to establish a person's exact position while indoors. *See, e.g.*, Michael Byrne, *New Indoor Positioning System Tracks Your Phone Using Sound Waves*, MOTHERBOARD, Apr. 2, 2016, http://bit.ly/2fEm5Wd; Tom Simonite, *Bringing Cell-Phone Location-Sensing Indoors*, MIT TECH. REV., Aug. 31, 2010, http://bit.ly/2fEJcA9.

[14] Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205, 217 (2015).

[15] Parmy Olson, *Algorithm Aims to Predict Crime by Tracking Mobile Phones*, FORBES, Aug. 6, 2012, http://bit.ly/2wzXDcO.

[16] *Id.* Sophisticated algorithms also stand to make it possible for CSLI to be used "to peek inside a person's mind and gauge mental health." Tom Simonite, *This Phone App Knows If You're Depressed*, MIT TECH. REV., Sept. 22, 2014, http://bit.ly/2w35PoW ("Motion, audio, and location data harvested from a smartphone can be analyzed to accurately predict stress or depression.").

by many names, including TriggerFish, StingRay, Gossamer, Harpoon, and Hailstorm.[17] These devices fool "nearby cell phones into believing that the device is a cell tower so that the cell phone's information is then downloaded into the [device]."[18] This ultimately allows the police to use CSLI "to determine, with a reasonable degree of certainty, . . . where an individual is located while a cell call is being placed."[19] And these devices are becoming more powerful all the time, with one of the latest iterations being a plane-mounted "two-foot-square box" that enables CSLI to be captured "from tens of thousands of cell phones" at a time.[20]

Taken together, the above points establish that Fourth Amendment analysis of CSLI must account for the ever more revealing nature of CSLI over time. Much like the thermal imager at issue in *Kyllo*, warrantless use of CSLI stands to permanently "erode the privacy guaranteed by the Fourth Amendment." 533 U.S. at 34. The Court should not leave individuals at "the mercy of [this] advancing technology." *Id.* at 36. The stakes are too high. "CSLI is only the tip of the iceberg when it comes to personal data that is now

---

[17] *See* Brian L. Owsley, *TriggerFish, StingRays, & Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 185 (2014).

[18] *Id.*

[19] *Id.* at 193.

[20] Jonathan Bard, *Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment*, 57 BOSTON COLLEGE L. REV. 731, 749–50 (2016).

routinely being collected by third parties."[21] The "relatively new Apple Watch," for example, "has the ability to track an individual much in the same way that smartphones can."[22] How the Court deals with CSLI will have a lasting influence on the privacy of information captured by many new technologies[23]—including those we cannot imagine yet.

III. The Court's Fourth Amendment analysis of CSLI should recognize that police use of CSLI comes with a high risk of abuse.

Fourth Amendment analysis requires the Court to be forward-looking not only in how it thinks about technology but also in how it thinks about the police. The Court "must remember the authority which [it] concede[s] to conduct" warrantless searches "may be exercised by the most unfit and ruthless officers as well as by the fit and responsible, and resorted to in

---

[21] WESLEY CHENG, CTR. FOR THE ADVANCEMENT OF PUBLIC INTEGRITY, COLUMBIA LAW SCHOOL, DOES SEEKING CELL SITE LOCATION INFORMATION REQUIRE A SEARCH WARRANT? 4 (2016), http://bit.ly/2uuCOSB.

[22] *Id.*

[23] *See, e.g., If These Walls Could Talk: The Smart Home & the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1924 (2017) ("Smart home technologies necessitate the sharing of personal information across a multitude of third-party service providers . . . ."); Natasha H. Duarte, *The Home Out of Context: The Post-*Riley *Fourth Amendment & Law Enforcement Collection of Smart Meter Data*, 93 N.C. L. REV. 1140, 1141 (2015) ("[S]mart meters take information about the activities that occur inside the home and put it in the hands of a third party—the utility company.").

case of petty misdemeanors as well as in the case of the gravest felonies." *Brinegar v. United States*, 338 U.S. 160, 182 (1949) (Jackson, J., dissenting). The Court must also remember that to the extent it grants any kind of authority to search, the police will be the first interpreters of this authority and they will push this authority "to the limit." *Id.*

On this score, the instances in which cell-site location information has been abused by the police are too numerous to count. Chief among these abuses has been police concealment of CSLI use from both the public and the courts themselves. For example, "[i]n one case after another, *USA Today* found police in Baltimore and other cities used the phone tracker, commonly known as a stingray, to locate the perpetrators of routine street crimes and frequently concealed that fact from the suspects, their lawyers and even judges."[24] This abuse was systematic and rampant: the police "used stingrays to catch everyone from killers to petty thieves" and then "regularly hid or obscured that surveillance once suspects got to court," such that "many of those they arrested were never prosecuted."[25]

Another police abuse of CSLI that has come to light in recent years is CSLI-based surveillance of romantic interests. Take the case of a Minnesota woman who obtained "a restraining order against her boyfriend, a state narcotics agent who she claimed abused

---

[24] Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA TODAY, Aug. 23, 2015, http://usat.ly/ 1JeqgNk.

[25] *Id.*

his access to cell-site data information to stalk her."[26] "She was granted the [restraining] order and the man is no longer a police officer."[27]

Of course, this kind of abuse is not confined to CSLI. As the *Washington Post* has found, "[t]here are plenty of cases in which local law enforcement officials have been accused of abusing their access to [police] databases to acquire information about potential romantic interests."[28] But this reality only underscores the extent to which police use of CSLI, free from Fourth Amendment restraints, increases the risk of abusive CSLI-based surveillance of romantic interests.

Finally, there are those CSLI abuses that have taken place abroad, demonstrating how CSLI can be used to "cow[] a population, crush[] the spirit of the individual and put[] terror in every heart." *Brinegar*, 338 U.S. at 180 (Jackson, J., dissenting). Amnesty International has compiled a devastating report on such abuses in the former Soviet state of Belarus.[29] Under

---

[26] Charles Blain, *Police Could Get Your Location Data Without a Warrant. That Has to End*, WIRED, Feb. 2, 2017, http://bit.ly/2jGGRkA.

[27] *Id.*; *see also* Mara H. Gottfried, *Minneapolis Officer Quits Amid Federal Probe of Metro Gang Strike Force*, PIONEER PRESS, Aug. 28, 2009, http://bit.ly/2vWk1is.

[28] Andrea Peterson, *LOVEINT: When NSA Officers Use Their Spying Power on Love Interests*, WASH. POST, Aug. 24, 2013, http://wapo.st/15kehuK.

[29] AMNESTY INT'L, "IT'S ENOUGH FOR PEOPLE TO FEEL IT EXISTS": CIVIL SOCIETY, SECRECY, & SURVEILLANCE IN BELARUS 6–8 (2016), http://bit.ly/2uuF7Fv.

Belarusian law, "mobile telephone [and] internet providers . . . are required to allow the authorities direct access to their customers' data."[30] This places Belarusians in constant fear of being tracked by the police through CSLI. For a Belarusian journalist, this has meant the frequent experience of "traveling to a town to meet activists with whom she had spoken on the phone, only to find that the police were waiting upon her arrival."[31] For a Belarusian human rights lawyer, this has meant being forced to suspect a "vehicle decked with antennae near protest events" was in fact "tracking protestors' phones."[32]

Troubling echoes of these fears also exist here at home. A freedom-of-information lawsuit against the Chicago Police Department has led to the production of public records establishing that Chicago has "spent more than $340,000 between 2005 and 2010 on cell-site simulators, as well as software upgrades and training."[33] "[The] fear is that police have been using the[se] devices to monitor protesters at events such as the NATO Summit. Demonstrators were suspicious that the batteries in their cellphones seemed to become

---

[30] *Id.* at 6.

[31] *Id.* at 21.

[32] *Id.*

[33] Frank Main, *Chicago Cops Lose Bid to Toss Lawsuit Over Secret Cell-Phone Tracking*, CHICAGO SUN-TIMES, Jan. 11, 2016, http://bit.ly/2uwZc9M.

quickly depleted during . . . protests—something caused by cell-tower simulators."[34]

Against this backdrop, with more and more police departments buying CSLI technology, the need to ensure this power is not abused has never been greater.[35] Any Fourth Amendment analysis of CSLI must account for this need. "It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon." *Boyd*, 116 U.S. at 635. That includes stealthy police use (and abuse) of CSLI.

CONCLUSION

Given the relational nature of privacy, the increasingly revealing nature of cell-site location information, and the high risk of CSLI abuse, the Court should hold that the Fourth Amendment governs CSLI. The Court should then find that "the question of what police must

---

[34] *Id.*

[35] *See* Jennifer Valentino-DeVries, *Police Snap Up Cheap Cellphone Trackers*, WALL ST. J., Aug. 19, 2015, http://on.wsj.com/2ux3Ep0.

do before searching [CSLI] . . . is accordingly simple—get a warrant." *Riley v. California*, 134 S. Ct. 2473, 2495 (2014).

Respectfully submitted,

MAHESHA P. SUBBARAMAN
Counsel of Record
SUBBARAMAN PLLC
222 S. 9th St., Ste. 1600
Minneapolis, MN 55402
(612) 315-9210
mps@subblaw.com

Counsel for Amicus Curiae Restore the Fourth, Inc.

Dated: August 14, 2017

RECORD AND BRIEFS

Supreme Court, U.S.
FILED
AUG 14 2017
OFFICE OF THE CLERK

No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Sixth Circuit

BRIEF OF *AMICUS CURIAE* THE RUTHERFORD INSTITUTE IN SUPPORT OF PETITIONER

JOHN W. WHITEHEAD
DOUGLAS R. MCKUSICK
THE RUTHERFORD INSTITUTE
P.O. Box 7482
Charlottesville, VA 22906
(434) 978-3888

D. ALICIA HICKOK
Counsel of Record
MARK D. TATICCHI
DRINKER BIDDLE & REATH LLP
One Logan Square
Philadelphia, PA 19103
(215) 988-2700
Alicia.Hickok@dbr.com

Counsel for Amicus Curiae

August 14, 2017

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

QUESTION PRESENTED

Whether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 127 days is permitted by the Fourth Amendment.

TABLE OF CONTENTS

	Page
QUESTION PRESENTED	i
TABLE OF AUTHORITIES	iv
INTEREST OF *AMICUS CURIAE*	1
INTRODUCTION AND SUMMARY OF ARGUMENT	2
ARGUMENT	2
I. THE COURT OF APPEALS FAILED TO ASSESS CONTEMPORARY EXPECTATIONS OF PRIVACY IN ITS FOURTH AMENDMENT ANALYSIS	2
II. THE COURT OF APPEALS FAILED TO FACTOR THE NATURE OF THE GOVERNMENT'S REQUEST INTO ITS FOURTH AMENDMENT ANALYSIS	10
CONCLUSION	15

TABLE OF AUTHORITIES

CASES — Page(s)

Corley v. *United States*,
556 U.S. 303 (2009) 13

Katz v. United States,
389 U.S. 347 (1967) 9

Kyllo v. *United States*,
533 U.S. 27 (2001) 9, 12

Smith v. *Maryland*,
442 U.S. 735 (1979) 3, 9

United States v. *Carpenter*,
819 F.3d 880 (6th Cir. 2016) 2, 3, 11, 14

United States v. *Jones*,
565 U.S. 400 (2012) 3, 4, 10

United States v. *Miller*,
425 U.S. 435 (1976) 3

CONSTITUTION

U.S. Const. amend. IV ..... *passim*

STATUTES

18 U.S.C. § 2703 ..... 2, 12, 13, 14

OTHER AUTHORITIES

Bank of America, U.S. Consumer Privacy Notice, https://www.bankofamerica.com/privacy/ consumer-privacy-notice.go (last visited Aug. 7, 2017) 8

TABLE OF AUTHORITIES—Continued

Page(s)

Facebook, Inc., Quarterly Report (Form 10-Q), *available at* http://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/dffb94d1-5a1b-4ec2-8eb7-56901be40efd.pdf 6, 7

Facebook.com, Privacy Basics, https://www.facebook.com/about/basics/usr1 (last visited Aug. 7, 2017) 4

Facebook.com, Privacy Basics: Deleting Posts, https://www.facebook.com/about/basics/manage-your-privacy/deleting-posts (last visited Aug. 7, 2017) 5

Facebook.com, Privacy Basics: Friend List, https://www.facebook.com/about/basics/manage-your-privacy/friend-list#1 (last visited Aug. 7, 2017) 5

Facebook.com, Privacy Basics: Likes & Comments, https://www.facebook.com/about/basics/manage-your-privacy/my-likes-and-comments#2 (last visited Aug. 7, 2017) 4-5

Facebook.com, Privacy Basics: Posts, https:// www.facebook.com/about/basics/manage-your-privacy/posts#11 (last visited Aug. 7, 2017) 5

Facebook.com, Privacy Basics: Profile, https://www.facebook.com/about/basics/manage-your-privacy/profile#6 (last visited Aug. 7, 2017) 5

TABLE OF AUTHORITIES—Continued

Page(s)

Facebook.com, Privacy Basics: Profile, https://www.facebook.com/about/basics/manage-your-privacy/profile #10 (last visited Aug. 7, 2017) 5

Facebook.com, Privacy Basics: Profile, https://www.facebook.com/about/basics/manage-your-privacy/profile#12 (last visited Aug. 7, 2017) 5

Google, Google+ Help: Using Circles on Google +, https://support.google.com/plus/answer/6320407?hl=en&ref_topic=6320382 (last visited Aug. 7, 2016) 6

Government of Canada, *Statistics Canada*, Sept. 28, 2016, http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/demo02a-eng.htm (last visited Aug. 9, 2017) 7

Instagram, How Do I Set My Photos and Videos to Private So That Only Approved Followers Can See Them?, https://help.instagram.com /448523408565555 (last visited Aug. 7, 2017) 6

InterContinental Hotels Group, InterContinental Hotels Group Privacy Policy, https://www.ihg.com/hotels/gb/en/global/customer_care/privacy_policy#4 (last visited Aug. 7, 2017) 8

TABLE OF AUTHORITIES—Continued

Page(s)

Kaiser Permanente, Privacy Statement, https://healthy.kaiserpermanente.org/health/care/consumer/ancillary/!ut/p/a1/hZBBj4IwEIV_iwfOM8pGgRuSuFZ0xWgEezEVG2xS26ZOzPLvVYxHw7tN5n1vMg84VMCNuKtGkLJG6NfMx8fZYrueTocprn_iCNkqm2fsL8enoIQF8EbbU2c-XIhcEmCAtTUkDXlpztJLHyDwmlonobopkkdntaqVvPUxZMT1w3Trf-pD_PuMt643XJ2hKosiSZbD_aScT1ZpHyLe4cLUSmvh2-f_vKsIQ7bpKvotxogsynf5Ps5DxNHH8EUpgrtGbajvS1lGFLNm8AAgXXxu/dl5/d5/L2DbisevZ 0FBIS9nQSEh/ (last visited Aug. 7, 2017) 8

LinkedIn, LinkedIn Help: Visibility of Your Updates, Posts, and Recent Activity, https://www.linkedin.com/help/linkedin/answer/ 61030 (last visited Aug. 7, 2017) 6

Macy's, Inc., Macy's and macys.com Notice of Privacy Practices, https://www.customerservice-macys.com/app/answers/detail/a_id/595/session/L2F2LzEvdGltZS8xNTAyMTUwMTAwL3NpZC9IWTdTLUFwbg%3D%3D#pref (last visited Aug. 7, 2017) 8

U.S. Census Bureau, *Population Distribution and Change: 2000 to 2010*, Mar. 2011, *avail-able at* https://www.census.gov/prod/cen2010/briefs/c2010br-01.pdf (last visited Aug. 9, 2017) 7

TABLE OF AUTHORITIES—Continued

Page(s)

Verizon, Privacy Policy for Fios and Other Fiber-to-the-Premises Customers, http://www.verizon.com/about/privacy/fios-privacy-policy (last visited Aug. 7, 2017)..... 8

INTEREST OF *AMICUS CURIAE*[1]

The Rutherford Institute is an international non-profit civil liberties organization headquartered in Charlottesville, Virginia. Founded in 1982 by its President, John W. Whitehead, the Institute provides *pro bono* legal representation to individuals whose civil liberties are threatened and educates the public about constitutional and human rights issues.

As part of its mission, The Rutherford Institute resists the erosion of fundamental civil liberties that many would ignore in a desire to enhance the ability of governmental authorities to detect, deter, and prosecute criminal activity. The Rutherford Institute believes that according ever increasing power and authority to law enforcement only creates a false sense of security while sanctioning unnecessary intrusions upon the private lives of private citizens.

The Rutherford Institute is interested in this case because it is committed to ensuring the continued vitality of the Fourth Amendment. Affirming the judgment of the Court of Appeals would undercut the Amendment's protections by enabling long-term surveillance of individuals—and the concomitant invasion of privacy that such surveillance entails—without first obtaining a warrant from a neutral magistrate.

---

[1] All parties to this matter have granted blanket consent for *amicus curiae* briefs in support of either or neither party. Petitioner filed such consent on July 11, 2017, and Respondent filed such consent on July 26, 2017. The requirements of Rule 37.2(a) of the rules of this Court are satisfied by these filings. No counsel for a party authored this brief in whole or in part, and no party or counsel for a party made a monetary contribution intended to fund the preparation or submission of this brief. No one other than *amicus curiae*, its members, or its counsel made a monetary contribution to the preparation or submission of this brief.

INTRODUCTION AND SUMMARY OF ARGUMENT

In addressing petitioner's Fourth Amendment challenge, the Court of Appeals framed the correct question: Did petitioner have a reasonable expectation of privacy in the 127 days' worth of cell-site location information the government obtained from his wireless carrier? See *United States* v. *Carpenter*, 819 F.3d 880, 886 (6th Cir. 2016).

The court went astray, however, in failing to properly contextualize that inquiry. *First*, it erred by failing to ask whether today, in the here and now, society would be prepared to accept petitioner's privacy expectations as reasonable.

Second, it failed to take account of the nature of the government's request—a demand for four months' worth of petitioner's movements—a factor which the text and structure of 18 U.S.C. § 2703 clearly contemplates being taken into account.

In light of these errors, the Sixth Circuit's judgment must be reversed.

ARGUMENT

I. THE COURT OF APPEALS FAILED TO ASSESS CONTEMPORARY EXPECTATIONS OF PRIVACY IN ITS FOURTH AMENDMENT ANALYSIS.

The Court of Appeals' decision in this case is the product of a flawed analytical framework. Rather than test petitioner's Fourth Amendment claim by assessing the present-day social and cultural expectations regarding the privacy of individuals' movements in public, the Sixth Circuit analogized the facts of this case to those of disparate decisions—often decades

old—that arose in a much different factual, social, legal, and technological context than that which prevails today. See *Carpenter*, 819 F.3d at 887-889 (citing, *inter alia*, *Smith* v. *Maryland*, 442 U.S. 735 (1979), and *United States* v. *Miller*, 425 U.S. 435, 443 (1976)). That was error.

Instead, the Court of Appeals should have straightforwardly applied the test that this Court's cases command: Did Timothy Carpenter possess a reasonable expectation that his (approximate) location and (general) movements would remain free from governmental oversight? Cf. *United States* v. *Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring in the judgment) ("The best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.").

If the Court of Appeals had not focused its analysis *exclusively* on the facts of prior cases and had instead also assessed *current* social understandings, it would have answered that query in the affirmative and held that a request for cell-site location data must, in the typical case, be supported by a warrant issued by a neutral magistrate upon a finding of probable cause.

The discussion that follows canvasses some of the contextual factors not considered by the Court of Appeals and explains why they compel the conclusion that petitioner's rights were traversed by the government's warrantless procurement of his cell-site location information.

1. The Court of Appeals erred by ignoring the significance of *present-day* social expectations in the Fourth Amendment analysis. As several Members of

this Court recognized only a few Terms ago, time and technology change the public's perception of what is—and should be—safe from prying governmental eyes. *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (invoking the "evolution of societal privacy expectations" in light of "technological advances"); *id.* at 427 (Alito, J., concurring in the judgment) ("Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes.").

In his concurrence in the judgment in *Jones*, Justice Alito posited one way in which technological change can shift that balance, suggesting that "[n]ew technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile." *Id.* at 427. People wishing to fly in an airplane, for example, agree to endure magnetometers, pat-down searches, and x-ray inspection of their luggage.

But the interaction between technology and expectations of privacy can also be less linear than the zero-sum tradeoff illustrated above might suggest. For example, technology can influence social understandings of how—and how broadly—an individual's information will be distributed when shared with a third party.

2. Social media provides a useful illustration. Take Facebook. The website's privacy guide assures users: "You have control over who sees what you share on Facebook." Facebook, Privacy Basics, https://www.facebook.com/about/basics/usr1 (last visited Aug. 7, 2017); Facebook, Privacy Basics: Likes & Comments, https://www.facebook.com/about/basics/manage-your-privacy/my-likes-and-comments#2 (last visited Aug. 7, 2017) ("The person who posts something has

control over the audience who can see it."). Thus, a Facebook user can publish information to a pre-populated list of recipients (*e.g.*, all individuals that the user has designated as "Close Friends") or create a customized list of recipients. Facebook, Privacy Basics: Posts, https://www.facebook.com/about/basics/manage-your-privacy/posts#11 (last visited Aug. 7, 2017); see also Facebook, Privacy Basics: Friend List, https://www.facebook.com/about/basics/manage-your-privacy/friend-list#1 (last visited Aug. 7, 2017) (informing users that they can restrict who may view a list of their Facebook contacts (*i.e.*, "friends")).

The website also allows users to see what their individual profile and pages look like—either to a class of other Facebook members (*e.g.*, members that are not designated as a "Friend" of the user) or to an individual Facebook member. Facebook, Privacy Basics: Profile, https://www.facebook.com/about/basics/manage-your-privacy/profile#6 (last visited Aug. 7, 2017). If the user learns that a third party can see information the user doesn't want that third party to see, that information can be restricted or deleted. Facebook, Privacy Basics: Profile, https://www.facebook.com/about/basics/manage-your-privacy/profile #10 (last visited Aug. 7, 2017). Similarly, if a Facebook user "post[s] something and later decide[s] [he or she] do[es]n't want people to see it, [the user] can delete it." Facebook, Privacy Basics: Deleting Posts, https://www.facebook.com/about/basics/manage-your-privacy/deleting-posts (last visited Aug. 7, 2017).

Indeed, users even have the ability to control who can see information about them that is posted by a *different* Facebook user. Facebook, Privacy Basics: Profile, https://www.facebook.com/about/basics/manage-your-privacy/profile#12 (last visited Aug. 7, 2017).

And that's just one social media site. Others afford users a similar degree of control over the information they share. See, *e.g.*, Google, Google+ Help: Use Circles on Google+, https://support.google.com/plus/answer/6320407?hl=en&ref_topic=6320382 (last visited Aug. 7, 2017) (explaining that users can add other Google+ members to a "circle"—*i.e.*, a collection of individuals who share something in common (being members of the user's family, fellow alumnae of her university, etc.)—and then choose which circle(s) will see each piece of information the user posts on Google+); Instagram, How Do I Set My Photos and Videos to Private So That Only Approved Followers Can See Them?, https://help.instagram.com/448523408565555 (last visited Aug. 7, 2017) (explaining that users can restrict access to a list of "followers" (*i.e.*, other Instagram members) whom the user must affirmatively approve before they can see information the user has posted to the social media site); LinkedIn, LinkedIn Help: Visibility of Your Updates, Posts, and Recent Activity, https://www.linkedin.com/help/linkedin/answer/61030 (last visited Aug. 7, 2017) (explaining that "[w]hen you share a post on your LinkedIn feed, you can choose whether to share your post publicly or to your connections only").

It is clear, moreover, that these media touch and affect an overwhelming number of the "people" with whom the Fourth Amendment is concerned. As of Q2 2017, Facebook alone boasted an average monthly user base of 236 million people in the U.S. and Canada. Facebook, Inc., Quarterly Report (Form 10-Q) at 22 (July 27, 2017), *available at* http://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/dffb94d1-5a1b-4ec2-8eb7-56901be40efd.pdf. In other words, even subtracting out one Facebook account for each of the

36.3 million residents of Canada,[2] that still leaves approximately 200 million accounts for the United States—nearly 65 percent of the country's population as of the last decennial census.[3]

3. In a similar vein, mobile phones and their applications ("apps") also offer users fine-grained control over dissemination of the users' information—and, in particular, the users' location information. Specifically, a user can decide which of the apps on his or her phone (if any) will be able to ascertain the phone's—and hence the user's—geographic location. See, *e.g.*, Apple, Inc., About Privacy and Location Services in iOS 8 and Later, https://support.apple.com/en-us/HT203033 (last visited Aug. 11, 2017) ("You can individually control which apps and system services have access to Location Services data.").

This allows users to exercise fully customizable control over the disclosure of their location information. So, for example, they may opt to allow the phone's ride-sharing (*e.g.*, Uber), navigation (*e.g.*, Google Maps), or weather apps to know where the user is located, but deny that information to social networking apps like Facebook or Instagram.

4. These contemporary expectations of nuanced control over the degree to which one's information will

---

[2] Government of Canada, *Statistics Canada*, Sept. 28, 2016, http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/demo02a-eng.htm (last visited Aug. 9, 2017).

[3] U.S. Census Bureau, *Population Distribution and Change: 2000 to 2010*, Mar. 2011, at 1, *available at* https://www.census.gov/prod/cen2010/briefs/c2010br-01.pdf (last visited Aug. 9, 2017). Were that not enough, Facebook also reports that, on each day during Q2 2017, an average of 183 million users logged onto its site. Facebook, Inc., Quarterly Report (Form 10-Q) at 21 (July 27, 2017).

be disseminated and the uses to which it will be put is not just a function of technology and the social media it has empowered. To the contrary, credit card issuers,[4] national retail chains,[5] global hotel conglomerates,[6] cable companies,[7] health care providers,[8] and countless other actors in the public sphere all disclose to individuals how and under what circumstances the information they provide may be shared with third parties—and how and to what extent the individual may limit further disclosure of that information (*e.g.*, by precluding a merchant from providing the individual's contact information to a third-party marketing organization).

---

[4] Bank of America, U.S. Consumer Privacy Notice, https://www.bankofamerica.com/privacy/consumer-privacy-notice.go (last visited Aug. 7, 2017).

[5] Macy's, Inc., Macy's and macys.com Notice of Privacy Practices, https://www.customerservice-macys.com/app/answers/detail/a_id/595/session/L2F2LzEvdGltZS8xNTAyMTUwMTAwL3NpZC9IWTdTLUFwbg%3D%3D#pref (last visited Aug. 7, 2017).

[6] InterContinental Hotels Group, InterContinental Hotels Group Privacy Policy, https://www.ihg.com/hotels/gb/en/global/customer_care/privacy_policy#4 (last visited Aug. 7, 2017).

[7] Verizon, Privacy Policy for Fios and Other Fiber-to-the-Premises Customers, http://www.verizon.com/about/privacy/fios-privacy-policy (last visited Aug. 7, 2017).

[8] Kaiser Permanente, Privacy Statement, https://healthy.kaiserpermanente.org/health/care/consumer/ancillary/!ut/p/a1/hZBBj4IwEIV_iwfOM8pGgRuSuFZ0xWgEezEVG2xS26ZOzPLvVYxHw7tN5n1vMg84VMCNuKtGkLJG6NfMx8fZYrueTocprn_iCNkqm2fsL8enoIQF8EbbU2c-XIhcEmCAtTUkDXlpztJLHyDwmlonobopkkdntaqVvPUxZMT1w3Trf-pD_PuMt643XJ2hKosiSZbD_aScT1ZpHyLe4cLUSmvh2-f vKsIQ7bpKvotxogsynf5Ps5DxNHH8EUpgrtGbajvS1lGFLNm8AAgXXxu/dl5/d5/L2dBISEvZ0FBIS9nQSEh/ (last visited Aug. 7, 2017).

5. The above examples highlight just a few facets of what a proper, modern-context-sensitive analysis would look to when attempting to ascertain the reasonableness of an individual's expectation of privacy in his or her cell-site location information. But even this subset of data points shows that societal understandings of privacy have changed significantly from the all-or-nothing concept of information disclosure that appears to undergird *Smith* v. *Maryland*, 442 U.S. 735 (1979), and its progeny. Today, technology has made it possible—and society has deemed it reasonable—for an individual to exert a more nuanced control over the information he or she discloses: *i.e.*, when, where, by whom, and for how long that information may be accessed.

That said, the immediate impact of these changes in societal expectations will be tempered somewhat by the circularity inherent in the *Katz* analysis. *See Kyllo* v. *United States*, 533 U.S. 27, 34 (2001). In other words, the *Katz* test has a locking-in effect: When the Court finds a practice does not trigger the warrant requirement, law enforcement may regularly engage in that process without securing a warrant—a practice that inherently undercuts any societal expectation of privacy in the information the government is securing. Thus, given *Smith*'s holding that the installation of a pen register is not a search, and the resulting ease with which such devices could be deployed, it remains highly unreasonable for an individual to expect such information to remain private.[9]

---

[9] The converse is also true: When the Court holds that a particular practice implicates a reasonable expectation of privacy, that perception of privacy is staunchly reinforced by (1) the reduction in occurrences that necessarily results from requiring a warrant; and (2) the knowledge that a neutral

* * *

In sum, the Court of Appeals failed to apply the methodology required by this Court's cases, eschewing a contemporary-society-based reasonable-expectation-of-privacy analysis (which would have accounted for, *inter alia*, modern technologies and the societal attitudes they impelled) in favor of a rote application of a rule that had its genesis in the heyday of the fax machine and thermal printer. Applying the wrong framework, the court below obtained the wrong answer. As shown above, the correct conclusion is that obtaining 127 days' worth of an individual's cell-site location data is a search within the meaning of the Fourth Amendment. The decision of the Court of Appeals for the Sixth Circuit should therefore be reversed.[10]

II. THE COURT OF APPEALS FAILED TO FACTOR THE NATURE OF THE GOVERNMENT'S REQUEST INTO ITS FOURTH AMENDMENT ANALYSIS.

The Court of Appeals failed to appreciate that the nature and extent of the government's actions—and the use to which that information would be put—had a bearing on its Fourth Amendment analysis. See *Jones*, 565 U.S. at 430-431 (2012) (Alito, J., concurring in the judgment) (contrasting "relatively short-term [GPS] monitoring of a person's movements on public streets," which likely would not qualify as a search,

---

magistrate and standard of probable cause have been interposed between an individual and the executive arm of the state.

[10] Alternatively, the Sixth Circuit's methodological error is, itself, sufficient grounds for vacating that court's decision and remanding this case so that the Court of Appeals may undertake the proper analysis of petitioner's claims.

with "the use of longer term GPS monitoring," which "impinges on expectations of privacy").

Here, the government sought 127 days' worth of petitioner's cell-site location information—effectively putting a retroactive tail on him for more than four months—in order to generate circumstantial evidence that he had, in fact, committed the crimes he was accused of committing. The long-term nature of that surveillance and purpose of gathering information for use in investigating and prosecuting a crime counsel strongly in favor of the conclusion that collection of petitioner's cell-site location information amounted to a search that required a warrant in order to proceed.[11]

The Sixth Circuit's counter-argument—that the information at issue is not specific enough to trench on privacy expectations—is both internally inconsistent and foreclosed by precedent. It is self-contradictory because, despite the supposed imprecision of the location information, it was proffered here—and has been proffered in many other cases—as competent evidence in support of a suspect's prosecution and conviction. *Carpenter*, 819 F.3d at 885; accord *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 311-312 (3d Cir. 2010) ("[T]he Government has asserted in other cases that a jury should rely on the accuracy of the cell tower records to infer that an individual, or at least her cell phone, was at home.");

---

[11] A different case might be presented, for example, if the government were to seek a narrower slice of information (*e.g.*, to confirm whether his phone was active or not) over a much more circumscribed period of time (*e.g.*, within a range of a few hours on a particular date) and for a different purpose (*e.g.*, to validate or challenge an alibi defense).

United States v. *Davis*, 785 F.3d 498, 540-541 (11th Cir. 2015) (en banc) (Martin, J., dissenting) (similar).

And the argument is foreclosed because this Court squarely rejected a parallel contention in *Kyllo*. In that case, the Court dismissed out of hand the notion that the lack of specificity in the data being gathered—a "crude visual image" from a thermal camera—precluded a finding that the use of the heat-sensing technology at issue qualified as a Fourth Amendment "search." *Id.* at 36-37. So too here, where the generalized nature of the location information at issue should not be held to insulate the government's collection efforts from the Fourth Amendment's warrant requirement.

Congress affirmed the importance of these contextual factors in its choice of text in Section 2703.

As relevant here, the statute provides:

> **(c) Records Concerning Electronic Communication Service or Remote Computing Service.—**
>
> (1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—
>
> (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant

> procedures) by a court of competent jurisdiction; [or]
>
> (B) obtains a court order for such disclosure under subsection (d) of this section; . . . .

Subsection (d), in turn, provides, in relevant part:

> (d) **Requirements for Court Order.**—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation. . . .

As this text makes plain, Congress mapped out two alternative paths to securing a subscriber's records from an electronic communications service provider: a warrant based on probable cause or a court order based on "reasonable grounds to believe that . . . the records . . . are relevant and material to an ongoing criminal investigation."

Put differently, unless Section 2703(c)(1)(A)'s warrant requirement is entirely superfluous, it must be the case that Congress contemplated that *sometimes* a request for such information would require a warrant, and *sometimes* it would not. Cf. *Corley* v. *United States*, 556 U.S. 303, 314 (2009) (rejecting broad reading of statutory exception to rule excluding certain confessions because that construction would have rendered a different—and narrower—exception provision "nonsensical and superfluous").

The Sixth Circuit's analysis overrides that congressional choice by making an impermissible generalization about the nature of the data that would *never* require a warrant. *Carpenter*, 819 F.3d at 887 ("The business records here fall on the unprotected side of this line. Those records say nothing about the content of any calls. Instead the records include routing information, which the wireless providers gathered in the ordinary course of business. Carriers necessarily track their customers' phones across different cell-site sectors to connect and maintain their customers' calls. And carriers keep records of these data to find weak spots in their network and to determine whether roaming charges apply, among other purposes. Thus, the cell-site data—like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves. The government's collection of business records containing these data therefore is not a search."). But, as explained above, that context-bereft analysis is consonant with neither the statutory text nor the Fourth Amendment backdrop against which Congress legislated.

Accordingly, because the Court of Appeals failed to heed the plain text and structure of Section 2703(c) in admitting evidence against Timothy Carpenter that was secured without a warrant, its judgment must be reversed.

CONCLUSION

For the foregoing reasons, the judgment of the Court of Appeals should be reversed.

Respectfully submitted,

JOHN W. WHITEHEAD
DOUGLAS R. MCKUSICK
THE RUTHERFORD INSTITUTE
P.O. Box 7482
Charlottesville, VA 22906
(434) 978-3888

D. ALICIA HICKOK
Counsel of Record
MARK D. TATICCHI
DRINKER BIDDLE & REATH LLP
One Logan Square
Philadelphia, PA 19103
(215) 988-2700
Alicia.Hickok@dbr.com

Counsel for Amicus Curiae

August 14, 2017

RECORD AND BRIEFS

No. 16-402

FILED
AUG 14 2017
OFFICE OF THE CLERK
SUPREME COURT, U.S.

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

—v.—

UNITED STATES OF AMERICA,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

BRIEF OF SCHOLARS OF CRIMINAL PROCEDURE AND PRIVACY AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

ANDREW G. FERGUSON
UDC DAVID A. CLARKE SCHOOL OF LAW
4340 Connecticut Avenue
Washington, D.C. 20008

HARRY SANDICK
Counsel of Record
KATHRINA SZYMBORSKI
JARED BUSZIN
PATTERSON BELKNAP WEBB & TYLER LLP
1133 Avenue of the Americas
New York, New York 10036
(212) 336-2000
hsandick@pbwt.com

Counsel for Amici Curiae

August 14, 2017

TABLE OF CONTENTS

Page

INTEREST OF *AMICI CURIAE* 1

SUMMARY OF ARGUMENT 2

ARGUMENT 3

I. EXTENSION OF *SMITH*'S REASONING WOULD POTENTIALLY EVISCERATE CITIZENS' PRIVACY IN THE DIGITAL AGE 3

A. Society's Relationship with Technology Has Changed Both Quantitatively and Qualitatively Since *Smith* 4

B. *Smith* Addressed a Radically Different Context Than This Case and Should Be Limited to Its Facts 8

II. THE THIRD-PARTY DOCTRINE HAS BEEN WIDELY CRITICIZED BY SCHOLARS 14

A. The Third-Party Doctrine Is Based on a Questionable Theory of Privacy 16

B. The Third-Party Doctrine Does Not Match Expectations of Privacy in the Digital Age 19

C. Justifications for the Third-Party Doctrine Do Not Hold Up in the Digital Age 21

CONCLUSION 27

TABLE OF AUTHORITIES

Page(s)

CASES

United States v. Benford,
2010 WL 1266507 (N.D. Ind. March 26, 2010) 10

Chapman v. United States,
365 U.S. 610 (1961) 23

Commonwealth v. Estabrook,
472 Mass. 852 (2015) 8

State v. Earls,
70 A.3d 630 (N.J. 2013) 9

Ferguson v. City of Charleston,
532 U.S. 67 (2001) 16

Georgia v. Randolph,
547 U.S. 103 (2006) 22

Hoffa v. United States,
385 U.S. 293 (1966) 17

United States v. Jeffers,
342 U.S. 48 (1951) 23

United States v. Jones,
565 U.S. 400 (2012) 6, 20

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

In re Application of the United States for an Order Authorizing the Installation & Use of a Pen Register & a Caller Identification System on Telephone Numbers, 402 F. Supp. 2d 597 (D. Md. 2005) 10

In re Application of the United States for Historical Cell Site Data, 2010 WL 4286365 (S.D. Tex. Oct. 29, 2010) 10

Katz v. United States, 389 U.S. 347 (1967) 3, 17, 18

Kyllo v. United States, 533 U.S. 27 (2001) 12

United States v. Maynard, 615 F. 3d 544 (D.C. Cir. 2010) 12

Packingham v. North Carolina, 137 S. Ct. 1730 (2017) 6

People v. Weaver, 12 N.Y.3d 433 (2009) 12, 13

Riley v. California, 134 S. Ct. 2473 (2014) 6, 7, 23, 24

Smith v. Maryland, 442 U.S. 735 (1979) ..... passim

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Stoner v. California,
376 U.S. 483 (1964) 23

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 20

STATUTES

18 U.S.C. § 2511(2)(a) 18

OTHER AUTHORITIES

Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 Vand. L. Rev. 1289 (1981) 15, 16

Jack M. Balkin, *Essay: The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1 (2008) 18

James Beck et al., *The Use of Global Positioning (GPS) and Cell Tower Evidence to Establish a Person's Location—Part II*, 49 Crim. Law. Bull. 8 (Summer 2013) 9

Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law*, 30 Harv. J.L. & Tech. 1 (2016) 20

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 Fordham L. Rev. 611 (2014) 17

Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & Pol'y 211 (2006) 18, 23

Nate Cardozo et al., *Who Has Your Back?: Protecting Your Data from Government Requests*, Elec. Frontier Found. (July 2017) 25

Brian Clark, *The Company Behind Roomba Cleaner Wants to Sell Home Data to Apple, Amazon, or Google*, Business Insider (July 25, 2017) 7

Sherry Colb, *What Is a Search: Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 Stan. L. Rev. 119 (2002) 18

Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 Calif. L. Rev. 1593 (1987) 23

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Chris Conley, *Non-Content Is Not Non-Sensitive: Moving Beyond the Content/non-Content Distinction*, 54 Santa Clara L. Rev. 821 (2014) 19

CTIA, *Annual Year-End 2016 Top-Line Survey Results*, https://www.ctia.org/docs/default-source/default-document-library/annual-year-end-2016-top-line-survey-results-final.pdf?sfvrsn=2 12

Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 Berkeley Tech. L.J. 1199 (2009) 21

Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. Pa. L. Rev. 327 (2015) 6

Andrew Guthrie Ferguson, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017) 22

Andrew Guthrie Ferguson, *The Smart Fourth Amendment*, 102 Cornell L. Rev. 547 (2017) 5

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681 (2011) 10

Susan Freiwald, *First Principles of Communications Privacy*, 2007 Stan. Tech. L. Rev. 3 (2007) 18

Government Accountability Office, Center for Science, Technology and Engineering, *Technology Assessment: Internet of Things, Status and Implication of an Increasingly Connected World*, GAO-17-75 (May 2017) 5

Government Requests Report, Facebook, https://govtrequests.facebook.com/country/United%20States/2016-H2/ 26

Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 Pepp. L. Rev. 975 (2007) 20

Stephen E. Henderson, *Carpenter v. United States and the Fourth Amendment: The Best Way Forward*, 26 William & Mary Bill of Rights J. (forthcoming 2017) 12

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373 (2006) 9

Stephen Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 Iowa L. Rev. Bull. 39 (2011) 18

Spenser Hsu, *Court: Warrantless Requests to Track Cellphones, Internet Use Grew Sevenfold in D.C. in Three Years*, Wash. Post (July 18, 2017)..... 13

Internet/Broadband Fact Sheet, Pew Research Center (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/internet-broadband/..... 4

Margot E. Kaminski, *Robots in the Home: What Will We Have Agreed To?*, 51 Idaho L. Rev. 661 (2015)..... 7

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. Rich. L. Rev 465 (2015) 14

Orin S. Kerr, *Applying the Fourth Amendment to Internet Communications: A General Approach*, 62 Stan. L. Rev. 1005 (2010) 25

Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561 (2009) 15, 21, 20

Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 Sup. Ct. Rev. 205 (2015)..... 15

Wayne R. La Fave, SEARCH AND SEIZURE, A TREATISE ON THE FOURTH AMENDMENT (5th ed. 2012) 16

Law Enforcement Requests, Lyft, https://help.lyft.com/hc/en-us/articles/214218437-Law-Enforcement-Requests 25

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 Mich. L. Rev. 1229 (1983) 19

Lyft Information Request Report – 2015, Lyft, https://lyft-assets.s3.amazonaws.com/helpcenter/Drive%20With%20Lyft/Lyft%20Transparency%20Report%20-%202015%20(1).pdf 26

Alex Matthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* (April 29, 2015) 14

Jonathan Mayer, Patrick Mutchler, & John C. Mitchell, *Evaluating the Privacy Properties of Telephone Metadata*, 113 PNAS 5536 (May 17, 2016) 7

Mobile Fact Sheet, Pew Research Center (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/ 4

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557 (2004) 18

OECD Digital Economy Outlook (Paris: OECD Publishing, 2015), http://dx.doi.org/10.1787/9789264232440-en 5

Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85 (2014) 5

Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934 (2013) 13

Jed Rubenfeld, *The End of Privacy*, 61 Stan. L. Rev. 101 (2008) 18

Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. Ill. J.L. Tech. & Pol'y 281 (2011) 22

Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 Cardozo L. Rev. 643 (2013) 20

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Christopher Slobogin, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007) 15, 18, 22

Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. Law Rev. 1083 (2002) 15, 18

Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 Md. L. Rev. 614 (2011) 20

Scott E. Sundby, *Everyman's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 Colum. L. Rev. 1751 (1994) 19

Matthew Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. 581 (2011) 5, 17, 23, 24

Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 Nw. U. L. Rev. 139 (2016) 11, 15

Transparency Report, Uber, https://transparencyreport.uber.com/ 26

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

James Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward An Expanded Vision of the Fourth Amendment Privacy Province*, 36 Hastings L.J. 645 (1985) 19

U.S. Department of Commerce Internet Policy Taskforce & Digital Economy Leadership Team, *Fostering the Advancement of the Internet of Things* (Jan. 2017) 4

Uber Guidelines for Law Enforcement Authorities, Uber, https://www.uber.com/legal/data-requests/guidelines-for-law-enforcement-united-states/en-US/ 25

Cleve R. Wootson, Jr., *A Man Detailed His Escape from a Burning House. His Pacemaker Told Police a Different Story*, Wash. Post (Feb. 8, 2017) 24

INTEREST OF *AMICI CURIAE*[1]

Amici curiae are forty-two scholars engaged in significant research and/or teaching on criminal procedure and privacy law. *See* Appendix A (listing individual scholars joining this brief). This brief addresses issues that are within *amici*'s particular areas of scholarly expertise. They have a shared interest in clarifying the law of privacy in the digital era, and believe that a review of scholarly literature on the topic is helpful to answering the question in this case.

---

[1] Pursuant to Rule 37.6, *amici curiae* certifies that this brief was not written in whole or in part by counsel for any party, and no person or entity other than *amici curiae* and its counsel has made a monetary contribution to the preparation and submission of this brief. Letters from the parties consenting to the filing of this brief have been filed with the Clerk of the Court.

SUMMARY OF ARGUMENT

This case presents an opportunity to reconsider the Fourth Amendment in the digital age. Cell phones are only one of the many new and pervasive digital technologies which automatically collect and reveal intimate personal data, such as Cell Site Location Information ("CSLI"), to third parties. This Court should resist extending the reasoning of *Smith v. Maryland*, 442 U.S. 735 (1979) -a 38-year-old case built on a faulty privacy premise—to the modern, hyper-connected, technology-dependent world. Instead, the Court should recognize that the new realities of this world require new legal doctrines to fit the privacy expectations shared by most Americans.

Criminal procedure and privacy scholars are in near-unanimous agreement that an extension of what some have called the "third-party doctrine," which holds that people lack a reasonable expectation of privacy in information voluntarily conveyed to third parties, could eliminate citizens' privacy in the modern age. CSLI (and other data transmitted to third parties in the modern age) can reveal an individual's interests, friendships, activities, travel, associations, beliefs, health concerns, financial problems, employment, and education. *Smith* is grounded in a pre-digital era, and cannot support future application of the Fourth Amendment.

The trajectory and pace of technological change further counsels against extending *Smith*. As the use of "smart" devices and their related applications steadily grows among Americans, so too does the volume, scope, detail, and type of intimate data

transmitted to third parties. An extension of *Smith*'s reasoning would give law enforcement ever-increasing access to the most private details of individuals' lives without a warrant or probable cause.

As a matter of Fourth Amendment practice, extending the third-party doctrine would curtail digital privacy and encourage arbitrary government intrusions into the lives of American citizens. As a matter of Fourth Amendment theory, applying the third-party doctrine to the digital world would undersell the value of privacy, and contradict the logic of *Katz v. United States*, 389 U.S. 347, 359 (1967) (1967) ("Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."). And, as a matter of precedent, *Smith* offers an inapposite and inadequate doctrinal foundation to support the future of a digital Fourth Amendment.

ARGUMENT

I. EXTENSION OF *SMITH*'S REASONING WOULD POTENTIALLY EVISCERATE CITIZENS' PRIVACY IN THE DIGITAL AGE

The Government and the Sixth Circuit both relied heavily on *Smith v. Maryland* in this case, drawing an analogy between the dialed phone numbers addressed in *Smith* and the CSLI addressed here. But the analogy is flawed on both technological and doctrinal grounds. Given the profound technological advances of the last 38 years—and

society's drastically changed relationship with technologies requiring third-party providers—upholding CSLI tracking on the basis of parallels to long-obsolete technology would lead to a substantial reduction in privacy in the modern era. This Court should limit the holding of *Smith* to its particular facts.

A. Society's Relationship with Technology Has Changed Both Quantitatively and Qualitatively Since Smith

The embrace of digital third-party services has quantitatively and qualitatively reshaped society's relationship with technology. The vast majority of Americans today are digital citizens—and reliance on connected devices is only growing. Pew Research Center reports that today 95 percent of adult Americans use cell phones, 90 percent use the Internet, 77 percent own smartphones, and 70 percent use social media.[2] The U.S. Department of Commerce Internet Policy Taskforce estimates that "between the years of 2015 and 2020, the number of connected devices in the United States will nearly double from 2.3 billion to 4.1 billion."[3] The

---

[2] *Mobile Fact Sheet*, Pew Research Ctr. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/; *Internet/Broadband Fact Sheet*, Pew Research Ctr. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/internet-broadband/.

[3] U.S. Department of Commerce Internet Policy Taskforce & Digital Economy Leadership Team, *Fostering the Advancement of the Internet of Things*, 4 (Jan. 2017), *available at* https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

Organisation for Economic Cooperation and Development ("OECD") reports that in OECD countries, including the United States, a family of four today has ten devices connected to the Internet in their household, with that number expected to grow to 50 devices by 2022.[4] Smart devices have proliferated inside Americans' homes, cars, and even their bodies.[5]

Virtually all these connected devices and their associated applications transmit information through third-party providers. All modern communication tools—including e-mail, text, cloud-based photo storage, Voice over Internet Protocol, iMessage, Twitter, Google chat, Instagram message, and many others—depend on cable, ISP, Bluetooth, phone, and Wi-Fi services run by third parties. *See* Matthew Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. 581, 602–04 (2011). Smartphones, smart homes, smart cars, and smart medical devices connected through the Internet of Things are only "smart" because of third-party interconnectivity. Andrew Guthrie Ferguson, *The Smart Fourth Amendment*, 102 Cornell L. Rev. 547, 557–59

---

[4] OECD Digital Economy Outlook, 255 (Paris: OECD Publishing, 2015), http://dx.doi.org/10.1787/9789264232440-en.

[5] Government Accountability Office, Center for Science, Technology and Engineering, *Technology Assessment: Internet of Things, Status and Implication of an Increasingly Connected World*, GAO-17-75, at 16–18 (May 2017); *see also* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85, 103–04 (2014) (discussing implantable health devices).

(2017). Millions of people share political and cultural opinions, news, and beliefs on third-party social media platforms. *See Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017). Internet searches and artificially intelligent assistants answer the most intimate and arcane questions through third-party search engines. *See United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (acknowledging the revealing nature of internet searches). Personal photographs, calendars, shopping lists, medical prescriptions, and an expanding network of contacts are housed in third-party storage. *See Riley v. California*, 134 S. Ct. 2473, 2491 (2014). Third-party data can be found in credit reports, employment histories, address changes, and retail purchases. Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. Pa. L. Rev. 327, 354–59 (2015). Families share their lives virtually, companies store their records electronically, and industries offer third-party technologies to service these expanding data-driven needs.

The ubiquity of third-party services has qualitatively changed our relationship with technology and each other. Indeed, one cannot effectively participate in the modern world without using these tools. To connect with friends, apply for jobs, receive medical services, or save photos from a family vacation, one must constantly transmit personal, "trackable" data to third-party services. Oftentimes these services collect location and other information through automation and without the user's knowledge or voluntary consent.

Third-party collection of intimate, personal data will only grow in the future. Companies have become adept at monetizing personal data, providing an ever-increasing incentive for them to collect more of it. Advances in connected technology will greatly expand the information that can be gleaned from data collected by third-party providers, going far beyond what is currently possible with CSLI data.[6] This will include the "content" of what is sent and saved, not merely the more neutral-seeming locational information that is at issue in this appeal.

The continuous data collection by smart devices and networks—from smart heating systems to smart heart stents—provides "a revealing montage of the user's life." *Riley*, 134 S. Ct. at 2490. For example, researchers have found that by simply studying vast sets of phone records they can predict who is in a relationship, sick, or involved in illicit activities.[7] Extending what some have called the third-party doctrine to digital third-party services could exempt all of this information from Fourth Amendment protection, potentially eliminating individual privacy in the modern age. *See* Margot E. Kaminski, *Robots in the Home: What Will We Have Agreed To?*, 51 Idaho L. Rev. 661, 670 (2015).

---

[6] *See* Brian Clark, *The Company Behind Roomba Cleaner Wants to Sell Home Data to Apple, Amazon, or Google*, Business Insider (July 25, 2017).

[7] Jonathan Mayer, Patrick Mutchler, & John C. Mitchell, *Evaluating the Privacy Properties of Telephone Metadata*, 113 PNAS 5536, 5540 (May 17, 2016).

B. Smith *Addressed a Radically Different Context Than This Case and Should Be Limited to Its Facts*

Smith was grounded in the particular context of dialed telephone numbers and mid-Twentieth-Century telephone routing. In *Smith*, the Court reasoned that Smith had no subjective expectation of privacy in the numbers he dialed because he very likely knew that the telephone company recorded the numbers of his long-distance phone calls. *Smith*, 442 U.S. at 742. His monthly bills revealed that the telephone company recorded his dialed phone numbers. *Id.* The telephone company also offered to check for overbilling and to identify callers making "annoying or obscene calls." *Id.* at 742–43. In short, because Smith affirmatively acted by dialing the phone numbers and had been informed repeatedly that the information was collected, he voluntarily conveyed the information to the third party, which in turn could choose to turn those numbers over to the government. *Id.* at 743–44. Nothing about the content of the communications was shared, only the identity of the individuals or businesses with whom a person communicated. *See id.*

When *Smith* was decided, society's relationship to technologies that transmitted information to third parties was very different than it is today.[8] The use

---

[8] Lower courts and states have struggled with the third-party doctrine in light of the increasing interconnectedness of modern society, with numerous jurisdictions rejecting its relevance to the modern era or limiting it to the facts of existing pre-digital-era cases. *See, e.g.*, *Commonwealth v. Estabrook*, 472 Mass. 852 (2015) (holding that a warrant was required to collect two weeks

of such tools was limited, and the transmission of information to third parties was clearly disclosed to users. *But see Smith*, 442 U.S. at 750 (Marshall J., dissenting) ("[U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. . . . It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."). More foundationally, the privacy implications of long-term, aggregated locational tracking from digital devices dwarf the privacy considerations in *Smith*. And extending *Smith*'s reasoning to define privacy today would have consequences beyond the criminal justice context, creating a chilling surveillance threat. Indeed, the differences between this case and *Smith* overwhelm any similarities.

First, as with all old-fashioned telephones, the user in *Smith* had to actively transmit numerical information to use the device (and thus reveal personal information). By contrast, cell phones can be tracked without the user making a call or sending a text. Cell phones periodically (roughly every 7 seconds) transmit a "registration" signal containing the phone's unique serial number. *See, e.g.*, James Beck et al., *The Use of Global Positioning (GPS) and Cell Tower Evidence to Establish a Person's Location—Part II*, 49 Crim. Law. Bull. 8 (Summer

---

of CSLI); *State v. Earls*, 70 A.3d 630 (N.J. 2013) (holding that a warrant was required to obtain cell phone tracking information); *see also* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373 (2006).

2013).[9] Simply by possessing a cell phone, an owner is revealing his or her location. This requires no affirmative act. Thus, CSLI cannot be analogized to *Smith*'s reasoning, which equated affirmative use (dialing a number) with a relinquishment of an expectation of privacy.

Second, *Smith* turned in large part on the Court's conclusion that the transmittal of information to a third party was "voluntary." *Smith*, 442 U.S. at 432–33; *but see id.* at 750 (Marshall J., dissenting). Today, cell phone users do not knowingly and voluntarily convey their location information to their cell phone companies. As a technological matter, the tracking is automatic and takes place between a phone and cell site without any volitional choice on the user's part. Indeed, recent empirical studies show that the majority of cell phone users do not even know that cell phone companies may be tracking and storing users' physical location via CSLI. One study found that only 26.5 percent of all cell phone users

---

[9] Registration data is routinely used by law enforcement. *See, e.g., In re Application of the U.S. for Historical Cell Site Data*, 2010 WL 4286365, at *1 (S.D. Tex. Oct. 29, 2010) ("[T]he Government seeks continuous location data to track the target phone over a two month period, whether the phone was in active use or not."); *United States v. Benford*, 2010 WL 1266507, at *1 (N.D. Ind. Mar. 26, 2010) (government sought information "identifying which cell tower communicated with the cell phone while it was turned on"); *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Numbers*, 402 F. Supp. 2d 597, 598 (D. Md. 2005) (government sought CSLI data identifying "the physical location of the person in possession of the cell phone whenever the phone was on."); *see also* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681, 705–08 (2011).

understand that their cell phone provider is tracking and storing information on their physical location. Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 Nw. U. L. Rev. 139, 175–79 (2016). Even fewer cell phone users are actually aware of cell-signal-based location tracking. When the minority of users who thought that tracking occurs was asked as a follow-up question to describe how their cell service provider collects information on their location, only 12.7 percent of these users gave a response that could be interpreted as referring to cell-site or cell-signal tracking. *Id.* at 177. Altogether, only 3.3 percent of all cell phone users surveyed gave responses that indicated awareness of CSLI tracking. *Id.* Cell phone users simply do not voluntarily convey any location information to their cell service providers and do not know that they are inadvertently conveying such information. This shared but mistaken belief by the general public that the possession of a cellphone does not submit someone to constant, recorded location tracking reflects the expectation of privacy that people have about their location information.

Third, location tracking is far more invasive than obtaining a monthly record of dialed numbers. CSLI tracking can reveal everywhere that a person goes for as long as he or she owns a cell phone—which, for most of us, will be the remainder of our adult lives. This data can track a person's movements with precision, and will become only more precise as technology improves, more cellular devices are used, and more cell towers are built.[10]

---

[10] When petitioner Timothy Carpenter's records were obtained in 2011, CSLI was already able to pinpoint a person's location

Information that reveals a person's location can reveal "trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the hy-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *People v. Weaver*, 12 N.Y.3d 433, 441–42 (2009). This information becomes even more revealing when aggregated and collected over long periods of time. *See United States v. Maynard*, 615 F. 3d 544, 562 (D.C. Cir. 2010) (*aff'd on other grounds sub nom Jones*, 565 U.S. 400). Service providers retain location data for long periods of time: AT&T for five years, Sprint for 18 months, and Verizon for one year. Pet. Br. at 20.

Location data therefore yields "a highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious, amicable and amorous, to name only a

---

within a .1 square mile area. Stephen E. Henderson, *Carpenter v. United States and the Fourth Amendment: The Best Way Forward*, 26 William & Mary Bill of Rights J. (forthcoming 2017), *available at* https://works.bepress.com/stephen_henderson/55/. Over the past decade, the number of cell sites has increased from 195,613 to 308,334, a trend that will only continue as an ever-increasing number of consumers demand ever-faster and more reliable cell service. *See* CTIA. *Annual Year-End 2016 Top-Line Survey Results*, https://www.ctia.org/docs/default-source/default-document-library/annual-year-end-2016-top-line-survey-results-final.pdf?sfvrsn=2 CSLI; *cf. Kyllo v. United States*, 533 U.S. 27, 36 (2001) ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.").

few—and of the pattern of our professional and avocational pursuits." *Weaver*, 12 N.Y. 3d at 442. Such data gives much more information about a person and his or her activities than does a list of phone numbers dialed. It is a modern-day panopticon of constant surveillance enabled by the necessary use of a cellphone.

Lastly, the data at issue here is distinguishable from that revealed in *Smith* because it has expressive value, and allowing law enforcement unfettered access to such information has far-reaching consequences beyond impacting privacy. An unchecked third-party doctrine creates a chilling surveillance threat that threatens associational liberty, free expression, and intellectual growth, undermining the democratic health of the nation. *See* Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934, 1936, 1940 (2013). Law enforcement's constitutionally unfettered access to every third-party data point means any citizen questioning the government—be they a journalist, judge, protestor, or pariah—will be at risk of being exposed through aggregated and collected personal third-party data. There is evidence that arbitrary, invasive, or overbroad requests of third-party providers have already proliferated, and will continue to do so without a constitutional check. *See* Spenser Hsu, *Court: Warrantless Requests to Track Cellphones, Internet Use Grew Sevenfold in D.C. in Three Years*, Wash. Post (July 18, 2017). The awareness that the government may at some point—even five years from now—review data revealing one's every movement will have chilling effects on controversial or even merely embarrassing conduct,

diminishing the ability of individuals to exercise their rights and freedoms. *See* Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. Rich. L. Rev 465, 474 (2015) (discussing studies that show changes in online user habits in response to public disclosure of government surveillance); Alex Matthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* (April 29, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/10/00023-97629.pdf (showing that Google searches for controversial topics decreased following the public revelation of the NSA's internet surveillance programs).

These crucial differences between *Smith* and this case apply to all smart devices. Most devices are designed to work automatically without user action, affirmatively thwarting the user's ability to make voluntary choices about information they choose to convey to third parties. These distinctions -and the threats to privacy and liberty posed by warrantless collection of data from third parties—will only be exacerbated as digital technology develops.

II. THE THIRD-PARTY DOCTRINE HAS BEEN WIDELY CRITICIZED BY SCHOLARS

For these reasons and others, almost every scholar to have written on the subject has called for the demise of the third-party doctrine enunciated in *Smith* as applied in the digital context. Many scholars have noted that the doctrine is based on a questionable theory of privacy, as most people do not

think of information disclosed to others for a limited purpose as no longer private for other purposes. *See, e.g.*, Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 Vand. L. Rev. 1289, 1315 (1981); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. Law Rev. 1083, 1135 (2002). Others have focused on the doctrine's inaptness to the expectations of privacy in the digital age. *See, e.g.*, Tokson, *Knowledge and Fourth Amendment Privacy*, 111 Nw. U. L. Rev. at 175–79; Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 Sup. Ct. Rev. 205 (2015); Christopher Slobogin, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 184–86 (2007). Although the doctrine has a vocal defender, *see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561 (2009),[11] the justifications offered do not hold up in the digital age. This Court should decline to extend the doctrine now, in line with the overwhelming weight of scholarly literature on the topic.

---

[11] Even Orin Kerr, the doctrine's chief defender, admits that "[i]t is the *Lochner* of search and seizure law, widely criticized as profoundly misguided." Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. at 563. Indeed, he notes, "[t]he verdict among commentators has been frequent and apparently unanimous: The third-party doctrine is not only wrong, but horribly wrong." *Id.*

A. The Third-Party Doctrine Is Based on a Questionable Theory of Privacy

The third-party doctrine's central tenet is that once an individual discloses information to any third party for any purpose, no matter how confidential, that citizen irrevocably sets aside any reasonable expectation that the government will not obtain that information from the third party without a warrant issued upon probable cause. This does not, however, accord with the expectations most people have when transmitting information for a specific purpose. As such, even setting aside the serious issues presented by the digital age, many scholars believe the third-party doctrine is based on a highly questionable premise.

Most people recognize that "[p]rivacy is not an all or nothing phenomenon." Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 Vand. L. Rev. at 1315; *Smith*, 442 U.S. at 749 (Marshall J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."). In disclosing information to a business, health care provider, or other third party, an individual has a reasonable expectation that his information will be used for a limited purpose and will not be disclosed to any other party without their permission. *See, e.g.*, Wayne R. La Fave, 1 SEARCH AND SEIZURE, A TREATISE ON THE FOURTH AMENDMENT § 2.7(c) (5th ed. 2012); *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001)

(concluding that hospital patients had a reasonable expectation of privacy in test results because the results were not disclosed to any other party without the patients' permission); *see also* Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 Fordham L. Rev. 611, 612 (2014) (arguing that when information is shared for the sole purpose of obtaining an indispensable social good, the third party's cooperation with law enforcement should be analyzed as a Fourth Amendment search). In particular, it is unreasonable to consider data somehow "not private" if the information, like CSLI, is generally exposed only to automated systems rather than human employees. *See* Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. at 611–27.

Moreover, the idea that the third-party doctrine applies even in cases where—like here—the government coerces a third party into disclosing such information is highly problematic. The doctrine was originally premised on the idea that individuals "assumed the risk" that an associate would choose to talk to the police. *See Hoffa v. United States*, 385 U.S. 293, 302 (1966). Allowing the police to coerce third parties into disclosing confidential information threatens to eliminate privacy in countless forms of personal information, and contradicts the reasoning of *Katz*—as surely it would have been a Fourth Amendment "search" if, in *Katz*, the government ordered the phone company to tap its own wires, even

though the company has the legal right to record phone conversations in several situations.[12]

As such, scholars and commentators overwhelmingly consider the third-party doctrine a perversion of the *Katz* test that fails to accurately consider either social norms or actual expectations of privacy. *See, e.g.*, Stephen Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 Iowa L. Rev. Bull. 39 (2011); Jed Rubenfeld, *The End of Privacy*, 61 Stan. L. Rev. 101, 113–14 (2008); Jack M. Balkin, *Essay: The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1, 19 (2008); Slobogin, PRIVACY AT RISK at 151–64; Susan Freiwald, *First Principles of Communications Privacy*, 2007 Stan. Tech. L. Rev. 3, 46–49 (2007); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & Pol'y 211, 242–44 (2006); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557, 1571 (2004); Sherry Colb, *What Is a Search: Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 Stan. L. Rev. 119 (2002); Daniel J. Solove, *Digital Dossiers*

---

[12] *See* 18 U.S.C. § 2511(2)(a)(i) ("It shall not be unlawful under this chapter for . . . an officer, employee, or agent of a provider of wire or electronic communication service . . . to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service."); *id.* § 2511(2)(a)(ii) (providing for telephone company compliance with law-enforcement requests).

and the Dissipation of Fourth Amendment Privacy, 75 S. Cal. Rev. 1083, 1093–94 (2002); Scott E. Sundby, *Everyman's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 Colum. L. Rev. 1751, 1757–58 (1994); James Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward An Expanded Vision of the Fourth Amendment Privacy Province*, 36 Hastings L. J. 645 (1985); Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 Mich. L. Rev. 1229, 1254–56 (1983).

B. The Third-Party Doctrine Does Not Match Expectations of Privacy in the Digital Age

Scholars have noted that the underlying assumptions behind the third-party doctrine concerning expectations of privacy and the consensual disclosure of information become even more misplaced in the digital age. Citizens have come to depend on third parties for vital services, and they lack adequate alternatives for these services. When engaging in everyday modern life, people do not expect that exposing personal information to one party means forgoing a reasonable expectation of privacy toward all others, including the police. As discussed above, few people are even aware that they are disclosing such information and on a vast and constant scale. Moreover, scholars have recognized that the artificial distinctions created as a compromise to avoid the privacy-destroying consequences of the third-party doctrine no longer work in the age of data. Chris Conley, *Non-Content Is Not Non-Sensitive: Moving Beyond the Content/non-Content Distinction*, 54 Santa Clara L.

Rev. 821, 831 (2014); Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz, Smith, *and Electronic Surveillance Law*, 30 Harv. J.L. & Tech. 1 (2016).

In particular, distinctions between public/private activities and content/non-content information fail to justify the third-party doctrine when applied to information sharing and long-term, aggregated, public surveillance. Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 Cardozo L. Rev. 643, 658 (2013); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 Pepp. L. Rev. 975, 1020–24 (2007). In certain circumstances, an aggregation of supposedly "non-content" location information can be as revealing as "content," just as public actions can reveal private expressive acts. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring). A full embrace of the third-party doctrine in the digital era would imply that individuals have no reasonable expectation of privacy in e-mails stored on third-party servers, electronic health records, and all third-party information linked to our smartphones. Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 Md. L. Rev. 614, 642 (2011); *see also United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (holding that the Fourth Amendment protects e-mail content).

Even isolated defenders of the third-party doctrine concede that justifying it on reasonable expectation of privacy grounds is "awkward and unconvincing," and assert that it is better conceptualized as a consent doctrine. Kerr, *The Case*

for the Third-Party Doctrine, 107 Mich. L. Rev. at 588. But this fallback argument of consent has itself been challenged as theoretically inadequate and practically inaccurate. Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 Berkeley Tech. L.J. 1199, 1206 (2009). And as a technological matter, in the context of CSLI and smart devices, the automated nature of ubiquitous and involuntary connection undercuts the consensual nature of the exposure.

The reality is this: There is no principled way to limit *Smith* once applied in the digital context. If *Smith* applies here, the proponents of warrantless CSLI cannot foreclose the extension of the third-party doctrine to authorize the disclosure of the content of our cyber-lives. The Court need not proceed down this path.

C. Justifications for the Third-Party Doctrine Do Not Hold Up in the Digital Age

The primary defender of the doctrine claims the rule is required for two reasons: first, to preserve a privacy/security balance built into the reasonable expectation of privacy test; and second, to develop clear *ex ante* rules for police to follow. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. at 584–85. Both justifications fall apart when applied to the invasive, precise, automatic, and involuntary data revealed to third parties in the digital age.

First, the technological landscape of the *Smith* era has been replaced by a world in which there exists an abundance of third-party data available to

law enforcement. The digital footprints we leave are extensive and exposing. If there is a need to rebalance the risks of privacy and security, the balance should shift toward limiting unfettered access to location data and other personal information. *See, e.g.*, Slobogin, PRIVACY AT RISK at 6–9; Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. Ill. J.L. Tech. & Pol'y 281, 285 (2011). In a world of big data policing, the ability to rummage among the available digital clues empowers law enforcement at the expense of citizens. Andrew Guthrie Ferguson, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 17–18, 129 (2017).

The second justification for the third-party doctrine turns on a stated need for *ex ante* clarity for law enforcement. Trying to divine exactly which information is protected in third-party business records is just too difficult, the argument goes. The third-party doctrine's simplistic answer is to assert that the individual loses all Fourth Amendment interest in the data shared with another party.

While clear, this solution is wrong and unnecessary. The better answer is that both the individual and the third party retain Fourth Amendment rights in the information produced and possessed by the individual, and the information produced and possessed by third parties. In a variety of circumstances—a renter living in a rented house, a package handed to a common courier, an e-mail on a third-party server—the Fourth Amendment recognizes that both owner and user have overlapping Fourth Amendment privacy rights. *See, e.g.*, *Georgia v. Randolph*, 547 U.S. 103, 114 (2006);

Chapman v. United States, 365 U.S. 610, 616-18 (1961); *Stoner v. California*, 376 U.S. 483, 489 (1964); *United States v. Jeffers*, 342 U.S. 48, 52 (1951); *see also* Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. at 630–31. The same should be true for digital information serviced by third parties. Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & Pol'y 211, 245–65 (2006); Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 Calif. L. Rev. 1593, 1593–1600 (1987). In fact, this duality is even more relevant in the digital age as the same information might be possessed simultaneously by the user and the third party. As the Court recognized in *Riley*, for example, information on a smart device may be stored locally and also on the cloud. *Riley*, 134 S. Ct. at 2491.

Allowing both user and third party to possess Fourth Amendment rights in this data would not create a logistical challenge for law enforcement. Even in the absence of the third-party doctrine, third-party service providers faced with government requests for user data would not need to calculate their users' Fourth Amendment rights. Just as in any other Fourth Amendment context, it is the government's responsibility to secure a warrant for an individual's personal data, whether stored by third-party services or otherwise.

So, for example, if the government wants to access collected data from a "smart" pacemaker to

investigate a crime,[13] the question is not who owns the digital content or who possesses the personal data, but what justification the police have for requesting the information.[14] Just like the other situations involving rental property, hotels, and couriers with overlapping privacy interests, law enforcement cannot merely ignore the privacy interests of one party by focusing on the other's ownership. Instead, because of the overlapping Fourth Amendment interests, police must get a warrant. This requirement offers equally clear *ex ante* "guidance to law enforcement through categorical rules." *See Riley*, 134 S. Ct. at 2491. While not simplistic, applying the traditional

---

[13] *See* Cleve R. Wootson, Jr., *A Man Detailed His Escape from a Burning House. His Pacemaker Told Police a Different Story*, Wash. Post (Feb. 8, 2017).

[14] Further, framing the argument about access to existing business records is a bit misleading. Be it CSLI or smart health data, these sought after digital "records" do not exist in some electronic filing cabinet of "records." The vast amount of digital information pinging from every cell tower and smart home is only seen by automated, computer collection systems and largely undifferentiated to the third-party collector. Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. at 604. To obtain specific information about a specific customer in response to a law enforcement request, the companies must affirmatively search the relevant datasets. If those datasets contain personal information (like the aggregated locational information of an individual) then the exposing, personal nature of the process becomes obvious. It is only by organizing the otherwise unanalyzed data that the relevant datasets get created. It is, thus, inaccurate to frame the issue as merely a request for business records from already created business data. The records—including personalized data—are created in response to a law enforcement request, and thus expose personal information in response to a law enforcement request.

reasonable expectation of privacy test and warrant requirement has been shown to work well enough and can be adapted to the digital age of locational tracking and smart devices.

Revealingly, a warrant requirement has been the default policy for major technology companies when it comes to requests for digital content held by third parties. Amazon, Apple, Dropbox, Facebook, Google, Lyft, Microsoft, Pinterest, Twitter, WordPress, and Yahoo among other third parties all require a lawful warrant to obtain the content of user data. *See* Nate Cardozo et al., *Who Has Your Back?: Protecting Your Data from Government Requests*, Elec. Frontier Found. 6–8, 12 (July 2017). To be precise, the company policies protect "content," nominally tracking the artificial content/non-content distinction between protected and unprotected communications being held by third parties. *See* Orin S. Kerr, *Applying the Fourth Amendment to Internet Communications: A General Approach*, 62 Stan. L. Rev. 1005, 1019–20 (2010). But, in practice, some companies' definition of "content" embraces location information and even shared public content. For example, the transportation company Lyft requires a warrant for "prospective cell tracking" (real-time tracking),[15] and Uber requires a warrant for GPS location information.[16] Third-party services like

---

[15] *Law Enforcement Requests*, Lyft, https://help.lyft.com/hc/en-us/articles/214218437-Law-Enforcement-Requests ("We will require a warrant for requests for content of communications between Users or for prospective location data.").

[16] *Uber Guidelines for Law Enforcement Authorities*, Uber, https://www.uber.com/legal/data-requests/guidelines-for-law-enforcement-united-states/en-US/ ("We require . . . [a] search

Facebook (which exists to share ideas, photos, and communications with others) still requires law enforcement to obtain a warrant before providing those shared ideas, photos, and location information to law enforcement.[17] The practice shows that consumers expect third parties to protect their personal information and that a warrant requirement for such information can be workable for companies and law enforcement.[18] This final point—that law enforcement manages to secure necessary data

---

warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel our disclosure of certain communications between people using Uber or GPS location information.").

[17] *Information for Law Enforcement Authorities*, Facebook, https://www.facebook.com/safety/groups/law/guidelines/, ("A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, timeline posts, and location information.").

[18] Facebook reported that the company received 14,736 warrant requests between July and December 2016, and that it provided some information 85.32 percent of the time. *Government Requests Report*, Facebook, https://govtrequests.facebook.com/country/United%20States/2016-H2/. Uber reported that the company received 205 warrant requests during the same time period, and that it provided some data 87 percent of the time. *Transparency Report*, Uber, https://transparencyreport.uber.com/. In 2015, the company received 16 search warrants, fully complied with 12, partially complied with three, and did not respond to one. *Lyft Information Request Report – 2015*, Lyft, https://lyft-assets.s3.amazonaws.com/helpcenter/Drive%20With%20Lyft/Lyft%20Transparency%20Report%20-%202015%20(1).pdf.

through warrants—demonstrates that a better balance between privacy and security can be struck.

CONCLUSION

The so-called third-party doctrine has been widely criticized by scholars for decades, and its underpinnings continue to erode. Both as a matter of privacy theory and due to practical concerns regarding today's technologies, the foundations no longer hold. Mechanical application of *Smith v. Maryland* to a digital age will undermine privacy and amplify mass surveillance in ways that threaten associational freedom and personal liberty. New technologies and new expectations of privacy require a new approach. To ensure that the Fourth Amendment protects privacy in the future as it has in the past, this Court should limit *Smith* to its unique facts, or otherwise reject the third-party doctrine outright.

Dated: August 14, 2017

Respectfully submitted,

ANDREW G. FERGUSON
UDC David A. Clarke School of Law
4340 Connecticut Ave.
Washington, D.C. 20008

HARRY SANDICK
Counsel of Record
KATHRINA SZYMBORSKI
JARED BUSZIN
Patterson Belknap Webb & Tyler LLP
1133 Avenue of the Americas
New York, NY 10036
(212) 336-2000
hsandick@pbwt.com

Counsel for *Amici Curiae*

APPENDIX A[19]

Barbara Babcock
Founder and former Director of the Public Defender Service in Washington, D.C.
Crown Professor of Law, Emerita
Stanford Law School

Jordan M. Blanke
Ernest L. Baskin, Jr. Distinguished Professor of Computer Information Systems and Law
Stetson School of Business & Economics
Mercer University

Robert M. Bloom
Professor of Law
Boston College Law School

Kiel Brennan-Marquez
Research Fellow, New York University School of Law
Visiting Fellow, Information Society Project, Yale Law School

Edwin J. Butterfoss
Professor of Law
Mitchell Hamline School of Law

Robert Calhoun
Professor of Law Emeritus
Golden Gate Law School

Adam Candeub

---

[19] *Amici curiae* appear in their individual capacities; institutional affiliations are provided here for identification purposes only.

Professor of Law
Director, IP, Information, & Communications Law Program
Michigan State University

Bennett Capers
Stanley A. August Professor of Law
Brooklyn Law School
Visiting Professor at Boston University School of Law (Fall 2017)

Jenny Carroll
Professor of Law
University of Alabama

Gabriel J. Chin
Edward L. Barrett Jr. Chair and Martin Luther King Jr. Professor of Law
UC Davis School of Law

Ralph D. Clifford
Professor of Law
University of Massachusetts Law School

Joshua Fairfield
William Donald Bain Family Professor of Law
Washington and Lee University

Andrew Guthrie Ferguson
Professor of Law
UDC David A. Clarke School of Law

James Grimmelmann
Professor of Law
Cornell Tech and Cornell Law School

Susan Freiwald
Associate Dean of Academic Affairs and Professor of Law
USF School of Law

Woodrow Hartzog
Professor of Law and Computer Science
Northeastern University
School of Law
College of Computer and Information Science

Janet C. Hoeffel
Catherine D. Pierson Professor of Law
Tulane University School of Law

David Jaros
Associate Professor of Law
University of Baltimore School of Law

Margot E. Kaminski
Associate Professor of Law
Colorado Law

Mark A. Lemley
William H. Neukom Professor
Stanford Law School

Dave Levine
Associate Professor
Elon University School of Law
Affiliate Scholar, Stanford Law School Center for Internet and Society

Richard H. McAdams
Bernard D. Meltzer Professor of Law
University of Chicago Law School

Thomas M. McDonnell
Professor of Law
Elisabeth Haub School of Law at Pace University

William McGeveran
Professor of Law and Solly Robins Distinguished Research Fellow
University of Minnesota Law School

Colin Miller
Professor and Associate Dean for Faculty Development
University of South Carolina School of Law

Steven J. Mulroy
Professor of Law
Humphreys School of Law, University of Memphis

Connie Davis Nichols
Professor of Law
Baylor Law School

Kenneth B. Nunn
Professor of Law
University of Florida, Levin College of Law

Paul Ohm
Professor of Law
Georgetown University Law Center

Brian L. Owsley
Assistant Professor of Law
UNT Dallas College of Law

Blake Reid
Associate Clinical Professor
Colorado Law

Neil Richards
Thomas & Karole Green Professor of Law
Washington University in St. Louis

David Rudovsky
Senior Fellow
Penn Law School

Jason Schultz
Professor of Clinical Law
New York University School of Law

Victoria L Schwartz
Associate Professor of Law
Pepperdine University School of Law

Dawinder S. Sidhu
Of Counsel, Shook, Hardy & Bacon, LLP
Visiting Professor, University of Baltimore School of Law

Priscilla J. Smith
Clinical Lecturer in Law
Director and Senior Fellow, Program for the Study of Reproductive Justice
Yale Law School

Randolph N. Stone
Clinical Professor of Law
University of Chicago Law School

Kim Taylor-Thompson
Professor of Clinical Law
New York University School of Law

George C. Thomas III
Rutgers University Board of Governors Professor of Law
Judge Alexander P. Waugh, Sr. Distinguished Scholar

Ari Ezra Waldman
Associate Professor of Law
New York Law School

Jonathan Weinberg
Professor of Law
Wayne State University

RECORD
AND
BRIEFS

Supreme Court, U.S.
FILED
AUG 14 2017
OFFICE OF THE CLERK

No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Sixth Circuit

BRIEF OF SCHOLARS OF THE HISTORY AND ORIGINAL MEANING OF THE FOURTH AMENDMENT AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

ELIZABETH B. WYDRA
BRIANNE J. GOROD*
BRIAN R. FRAZELLE
CONSTITUTIONAL
ACCOUNTABILITY CENTER
1200 18th Street NW, Suite 501
Washington, D.C. 20036
(202) 296-6889
brianne@theusconstitution.org

Counsel for Amici Curiae

August 14, 2017

* Counsel of Record

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES	ii
INTEREST OF *AMICI CURIAE*	1
INTRODUCTION AND SUMMARY OF ARGUMENT	2
ARGUMENT	6
I. Seeking the Whereabouts of a Person or Her Effects by Examining Cell Site Location Information Is a "Search"	6
II. The Right of The People To Be Secure in Their Persons and Effects Against Unreasonable Searches Is Violated When the Government Has Unfettered Power To Track The People's Whereabouts Through Their Cell Phone Records	14
III. The Stored Communications Act's Protections Are Inadequate	28
CONCLUSION	32

TABLE OF AUTHORITIES

Page(s)

Cases

ACLU v. Clapper,
959 F. Supp. 2d 724 (S.D.N.Y. 2013) 30

Arizona v. Hicks,
480 U.S. 321 (1987) 13

Bell v. Clapp,
10 Johns. 263 (N.Y. Sup. Ct. 1813) 21

Boyd v. United States,
116 U.S. 616 (1886) 7, 8, 10

Brinegar v. United States,
338 U.S. 160 (1949) 17

Camara v. Mun. Ct.,
387 U.S. 523 (1967) 17

City of Ontario v. Quon,
560 U.S. 746 (2010) 25

Coolidge v. New Hampshire,
403 U.S. 443 (1971) 29

District of Columbia v. Heller,
554 U.S. 570 (2008) 16

Entick v. Carrington,
19 How. St. Tr. 1029 (1765) 8, 10, 18-19

Ex parte Siebold,
100 U.S. 371 (1879) 13

Frisbie v. Butler,
1 Kirby 213 (Conn. Super. Ct. 1787) 20

TABLE OF AUTHORITIES – cont'd

Page(s)

Go-Bart Importing Co. v. United States,
282 U.S. 344 (1931) 28

Goldman v. United States,
316 U.S. 129 (1942) 11

Grumon v. Raymond,
1 Conn. 40 (1814) 21

Huckle v. Money,
95 Eng. Rep. 768 (1763) 19

In re F.B.I. App. for an Order Requiring Prod. of Tangible Things, No. BR 13-109, 2013 WL 5741573 (FISA Ct. Aug. 29, 2013) 30

Interstate Commerce Comm'n v. Brimson,
154 U.S. 447 (1894) 10

Katz v. United States,
389 U.S. 347 (1967) 3, 12, 22

Kyllo v. United States,
533 U.S. 27 (2001) ..... *passim*

Johnson v. United States,
333 U.S. 10 (1948) 5, 29

Minnesota v. Carter,
525 U.S. 83 (1998) 13

Money v. Leach,
97 Eng. Rep. 1075 (1765) 18

Olmstead v. United States,
277 U.S. 438 (1928) 10-11

TABLE OF AUTHORITIES – cont'd

	Page(s)
Rakas v. Illinois, 439 U.S. 128 (1978)	13, 15
Riley v. California, 134 S. Ct. 2473 (2014)	*passim*
Smith v. Maryland, 442 U.S. 735 (1979)	12, 22, 26
State of Tennessee v. Whitworth, 117 U.S. 139 (1886)	6
United States v. Davis, 785 F.3d 498 (11th Cir. 2015)	30
United States v. Di Re, 332 U.S. 581 (1948)	17
United States v. Jones, 565 U.S. 400 (2012)	*passim*
United States v. Karo, 468 U.S. 705 (1984)	11, 31
United States v. Knotts, 460 U.S. 276 (1983)	5, 21, 23-24, 26
United States v. S.-E. Underwriters Ass'n, 322 U.S. 533 (1944)	6
United States v. Verdugo-Urquidez, 494 U.S. 259 (1990)	7, 16
United States v. Warshak, 631 F.3d 266 (6th Cir. 2010)	11
Wilkes v. Wood, 98 Eng. Rep. 489 (1763)	3, 9, 18

TABLE OF AUTHORITIES – cont'd

Page(s)

Wolf v. Colorado,
338 U.S. 25 (1949) 17

Constitutional and Statutory Provisions

U.S. Const. amend. IV 3, 9, 15, 28

Mass. Const. pt. 1, art. XIV (1780) 16

Penn. Const. art. X (1776) 16

18 U.S.C. § 2703(c) 5, 31

18 U.S.C. § 2703(d) 29

50 U.S.C. § 1861(b) 30

Books, Articles, and Other Authorities

The Conductor Generalis: or, the Office, Duty, and Authority of Justices of the Peace (1792) 7

William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning 602–1791* (2009) 8, 19

Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich. L. Rev. 547 (1999) 15, 16, 28

Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181 (2016) 3, 15, 18, 19

David Gray, *The Fourth Amendment in an Age of Surveillance* (2017) 4-5, 15, 18, 23

TABLE OF AUTHORITIES – cont'd

Page(s)

David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 Minn. L. Rev. 62 (2013) 22

2 Matthew Hale, *Pleas of the Crown* (1736) ... 14

Samuel Johnson, *A Dictionary of the English Language* (10th ed. 1792) ..... *passim*

Magistrate Report, *in* London J. (Apr. 24, 1731) 8

2 Francis Maseres, *The Canadian Freeholder: In Three Dialogues Between an Englishman and a Frenchman* (1779) 20

Luke M. Milligan, *The Forgotten Right To Be Secure*, 65 Hastings L.J. 713 (2014) 17, 19, 29

Order, 17 Jan. 1705/6 *in* 3 Buckinghamshire Sessions Records (Le Hardy ed., 1939) 8

James Otis, *In Opposition to Writs of Assistance* (1761) 3, 19-20

William Sheppard, *The Offices of Constables* (4th ed. 1658) 7

Noah Webster, *An American Dictionary of the English Language* (1828) 6, 7, 12

INTEREST OF *AMICI CURIAE*[1]

The following scholars are experts on the history and original meaning of the Fourth Amendment. *Amici* have published books or law review articles on the subject and teach courses in constitutional law, criminal procedure, and other topics:

Danielle Citron, Morton & Sophia Macht Professor of Law, University of Maryland Carey School of Law

Morgan Cloud, Charles Howard Candler Professor of Law, Emory University

Bradford Colbert, Resident Adjunct Professor, Mitchell Hamline School of Law

Dr. William Cuddihy, Adjunct Associate Professor of History, Los Angeles City College

Laura K. Donohue, Professor of Law, Georgetown Law

Norman M. Garland, Professor of Law, Southwestern Law School

David Gray, Professor of Law, University of Maryland Carey School of Law

Margaret Hu, Assistant Professor of Law, Washington and Lee University School of Law

---

[1] The parties have consented to the filing of this brief and their letters of consent have been filed with the Clerk. Under Rule 37.6 of the Rules of this Court, *amici* state that no counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than *amici* or their counsel made a monetary contribution to its preparation or submission.

Renée McDonald Hutchins, Jacob A. France Professor of Public Interest Law, University of Maryland Carey School of Law

Tracey Maclin, Professor of Law, Boston University School of Law

Luke Milligan, Professor of Law, Louis D. Brandeis School of Law, University of Louisville

George C. Thomas III, Board of Governors Professor of Law and Judge Alexander P. Waugh, Sr. Distinguished Scholar, Rutgers School of Law[2]

INTRODUCTION AND SUMMARY OF ARGUMENT

Law enforcement officials wanted to learn where Petitioner Timothy Carpenter was at the time of certain robberies. To figure that out, they obtained records from his cellular service provider showing the movements of his cell phone. Examining those records, they were able to track Carpenter's whereabouts over a four-month period.

Obtaining and examining those records was a "search" in any normal sense of the word—a search of documents and a search for Carpenter and one of his personal effects. It was therefore a "search" within the meaning of the Fourth Amendment. When the Amendment was ratified, to "search" meant to "examine," "explore," "look through," "inquire," "seek," or "try to find." Samuel Johnson, *A Dictionary of the English Language* (10th ed. 1792). Nothing about the text of the Fourth Amendment, or the historical backdrop against which it was adopted, suggests that the term "search" should be construed more narrowly in that Amendment to mean only conduct violating "an actual

---

[2] Institution names are provided for purposes of affiliation only.

(subjective) expectation of privacy" that "society is prepared to recognize as 'reasonable.'" *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Plainly, by examining and looking through Carpenter's cell site location records to seek the whereabouts of his person and phone, the government agents in this case conducted a "search."

Entrusting government agents with unfettered discretion to conduct searches using cell site location information undermines Fourth Amendment rights. The Amendment guarantees "*[t]he right of the people to be secure* in their persons, houses, papers, and effects, against unreasonable searches." U.S. Const. amend. IV (emphasis added). The Framers chose that language deliberately. It reflected the insecurity they suffered under the British at the hands of "writs of assistance," a form of general warrant that granted state agents broad discretion to search wherever they pleased. Such arbitrary power was "unreasonable" to the Framers, being "against the reason of the common law," Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181, 1270 (2016), and it was intolerable because of its oppressive impact on "the people" as a whole. As emphasized in one of the seminal English cases that inspired the Amendment, this kind of general power to search was "totally subversive of the liberty of the subject." *Wilkes v. Wood*, 98 Eng. Rep. 489, 498 (1763). James Otis's famous speech denouncing a colonial writ of assistance similarly condemned those writs as "the worst instrument of arbitrary power," placing "the liberty of every man in the hands of every petty officer." James Otis, *In Opposition to Writs of Assistance* (1761), *available at* http://hartleby.com/268/8/9.

Thus, although those who drafted and ratified the Fourth Amendment could not have anticipated cell-phone technology, they would have recognized the dangers inherent in any state claim of unlimited authority to conduct searches for evidence of criminal activity. Cell site location information provides insight into where we go and what we do—potentially revealing one's intimate relationships, hobbies, predilections, medical conditions, religious beliefs, and political pursuits. Because this information is constantly generated and can be retrieved by the government long after the activities it memorializes have taken place, unfettered government access to cell site location information raises the specter of general searches and undermines the security of "the people."

The use of more primitive techniques to track a person's movements, such as live visual surveillance in public spaces, does not pose the same threat to the security of the people. Traditional methods require considerable time and resources, making their use limited and infrequent. "The people" can therefore remain secure in their persons and effects against the fear that police might track their movements without a compelling reason to do so. *See United States v. Jones*, 565 U.S. 400, 429 (2012) (Alito, J., concurring in the judgment) ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical.").

Today, however, ubiquitous personal electronic devices generate perpetual records of almost everyone's movements, "mak[ing] long-term monitoring [of the people] relatively easy and cheap." *Id.* These developments have fundamentally transformed the state's capacity to track and monitor the people. David Gray, *The Fourth Amendment in an Age of Surveillance* 124

(2017) ("[W]hat is troubling about life in our age of surveillance is the prospect of living in a world where each of us and all of us are subject to the constant and real threat of broad and indiscriminate surveillance."). And if left unchecked, such developments will "alter the relationship between citizen and government in a way that is inimical to democratic society." *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (citation omitted).

Searches conducted using cell site location information raise precisely this danger. Today, "it is the person who is not carrying a cell phone . . . who is the exception," *Riley v. California*, 134 S. Ct. 2473, 2490 (2014), and "nearly three-quarters of smart phone users [have] report[ed] being within five feet of their phones most of the time." *Id.* All of these "cell-phone user[s] *must* reveal [their] general location to a cell tower in order for the cellular service provider to connect a call." Cert. Opp. 15 (emphasis added). Because anyone who uses this basic tool of modern life has no choice but to create a perpetual digital trail of his or her movements, the rise of modern cell phones has effectively enabled "twenty-four hour surveillance of any citizen of this country." *United States v. Knotts*, 460 U.S. 276, 283 (1983). Unfettered government access to that data is incompatible with "a society which chooses to dwell in reasonable security and freedom from surveillance." *Johnson v. United States*, 333 U.S. 10, 14 (1948).

Although the procedures set forth in the Stored Communications Act ("SCA") may limit the government's access to cell site location information, *see* 18 U.S.C. § 2703(c), the Act was passed long before access to telephone records allowed comprehensive tracking of subscribers' movements. As a consequence,

the SCA does not require sufficiently rigorous justifications for government access to this revealing data. Neither does the Act adequately limit the breadth of searches conducted using cell site location information. That shortcoming is evident in this case, where investigators needed location information only for specific times and dates, Pet. App. 6a, but requested and received location data covering more than four months, Pet'r Br. 6-7 & n.4; *see* Pet. App. 52a. Because of these flaws, the SCA does not sufficiently guard against threats of unreasonable searches and seizures.

ARGUMENT

I. Seeking the Whereabouts of a Person or Her Effects by Examining Cell Site Location Information Is a "Search"

A. "Words in a constitution . . . are always to be given the meaning they have in common use, unless there are very strong reasons to the contrary." *State of Tennessee v. Whitworth*, 117 U.S. 139, 147 (1886). "Ordinarily courts do not construe words used in the Constitution so as to give them a meaning more narrow than one which they had in the common parlance of the times in which the Constitution was written." *United States v. S.-E. Underwriters Ass'n*, 322 U.S. 533, 539 (1944).

"When the Fourth Amendment was adopted, as now, to 'search' meant '[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book; to *search* the wood for a thief.'" *Kyllo v. United States*, 533 U.S. 27, 32 n.1 (2001) (quoting Noah Webster, *An American Dictionary of the English Language* (1828)); *see* Johnson, *A Dictionary of the English Language*, *supra* (defining "search" as to "examine," "explore," "look

through," "inquire," "seek," or "try to find" by "looking into every suspected place").

Nothing about the text of the Fourth Amendment or the historical context in which it was adopted suggests that the word "searches" should be construed more narrowly in that Amendment. The Fourth Amendment "was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity," *Riley*, 134 S. Ct. at 2494, "often to uncover papers that might be used to convict persons of libel." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 266 (1990); *see Boyd v. United States*, 116 U.S. 616, 625-26 (1886). These quests for smuggled goods, seditious materials, and the people responsible were "searches" in the ordinary sense of the word—efforts to find persons and things.

Nor was the word "search" reserved in eighteenth-century America for activities that involved crossing the threshold of a home or business. For example, the word had long been used to describe efforts by law enforcement to find people in public places. *See, e.g.*, Webster, *supra* ("to *search* the wood for a thief"); William Sheppard, *The Offices of Constables*, ch. 8, § 2 (4th ed. 1658) ("The Officer receiving a Hue and Cry after a Fellon, must, with all speed, make diligent pursuit, with Horse and Foot, after the offendors from Town to Town the way it is sent, and make diligent search in his own Town."); *The Conductor Generalis: or, the Office, Duty, and Authority of Justices of the Peace* 187-88 (1792) (noting the authority of a constable or sheriff to "search in his town for suspected persons" and advising that "it is a good course to have the warrant of a justice of the peace, when time will permit, in order

to prevent causeless hue and cry"); William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning 602–1791*, at 320 (2009) (citing English magistrate's order commanding officers "to make diligent search" for able-bodied vagrants (quoting Order, 17 Jan. 1705/6 *in* 3 Buckinghamshire Sessions Records (Le Hardy ed., 1939))); *id.* at 322 (citing English magistrates' report describing "Rogues, Vagabonds, sturdy Beggars, and disorderly Persons apprehended by virtue of search Warrants[,] in Night Houses and other disorderly Houses or such as infest the Streets in the Night-time" (quoting *Magistrate Report, in* London J., at 2 (Apr. 24, 1731))).

As it does today, the word "search" when used in 1791 also encompassed the perusal and inspection of documents for the information they contained. Indeed, the government's pursuit of seditious writings was at the very heart of the English general warrant cases, those "landmarks" of freedom that were "applauded by the lovers of liberty in the colonies." *Boyd*, 116 U.S. at 626. In *Entick v. Carrington*, a case "undoubtedly familiar" to "every American statesman, during our revolutionary and formative period as a nation," *id.* at 626, the King's Bench rejected the notion that libelous materials "may be searched for and seized by whomsoever and wheresoever the Secretary of State thinks fit," condemning general warrants to "enter a man's house, search for and take away all his books and papers." *Entick v. Carrington*, 19 How. St. Tr. 1029 (1765). Pronouncing these searches unlawful, Lord Camden emphasized that the essence of the offense was not the physical confiscation of such documents, but rather state agents' reading and examining them. Papers, he explained, are the owner's "dearest property," which "will hardly bear an inspection." *Id.* at 1066.

B. Eighteenth-century readers would not have regarded physical intrusions as necessary elements of the "searches" addressed in the Fourth Amendment. True, "[t]he text of the Fourth Amendment reflects its close connection to property, since otherwise . . . the phrase 'in their persons, houses, papers, and effects' would have been superfluous." *Jones*, 565 U.S. at 405. But the same text reveals that the Amendment does more than simply protect those listed items from physical intrusion. If that were the Amendment's sole aim, it would merely prohibit "unreasonable searches of persons, houses, papers, and effects." Instead, it prohibits violations of "*[t]he right of the people to be secure* in their persons, houses, papers, and effects, against unreasonable searches." U.S. Const. amend. IV (emphasis added). And that "right . . . to be secure" can be violated by means other than a physical intrusion.

In the material conditions of the eighteenth century, few searches were capable of violating the security of persons, houses, papers, or effects without also physically intruding upon them. But even in the eighteenth century, jurists and statesmen who opposed general warrants made clear that their concerns went beyond physical intrusion to include the dangers of the state accessing *information* and prying into personal matters.

In the celebrated case *Wilkes v. Wood*, for instance, the plaintiff complained that his "papers had undergone the inspection of very improper persons to examine his private concerns," and maintained that "of all offences that of a seizure of papers was the least capable of reparation; that, for other offences, an acknowledgement might make amends; but that for the promulgation of our most private concerns, affairs of the most secret personal nature, no reparation whatsoever could be made." 98 Eng. Rep. at 498, 490.

In *Entick v. Carrington*, it was similarly charged that the defendants had "read over, pried into, and examined all the private papers, books, etc. of the plaintiff . . . whereby the secret affairs, etc. of the plaintiff became wrongfully discovered." 19 How. St. Tr. 1029. Pronouncing this conduct unlawful, Lord Camden explained that "the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass." *Id.* at 1066.

This Court later distilled the principles set forth in *Entick*, a case "in the minds of those who framed the fourth amendment to the constitution" and "considered as sufficiently explanatory of what was meant by unreasonable searches and seizures." *Boyd*, 116 U.S. at 626-27. "It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense," this Court explained. "The principles laid down in this opinion," reaching beyond "the concrete form of the case then before the court," condemn "the invasion of his indefeasible right of personal security" and the "privacies of life" when "that right has never been forfeited by his conviction of some public offense." *Id.* at 630; *see Interstate Commerce Comm'n v. Brimson*, 154 U.S. 447, 479 (1894) ("the right of personal security . . . involves, not merely protection of [a] person from assault, but exemption of his private affairs . . . from the inspection and scrutiny of others").

In the eighteenth century, little information could be gained about the activities inside a home without entering it. And because information could be memorialized only on objects palpable to the touch, "[f]orce and violence were then the only means known" to wrest private knowledge from its possessor. *Olmstead*

v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting). But "science has brought forth far more effective devices" than those available at the Founding. *Goldman v. United States*, 316 U.S. 129, 139 (1942) (Murphy, J., dissenting). Tools like thermal imagers and electronic trackers can acquire "information regarding the interior of the home that could not otherwise have been obtained" without physical intrusion. *Kyllo*, 533 U.S. at 34-35; *see United States v. Karo*, 468 U.S. 705, 715 (1984). Modern equivalents of traditional "papers," such as audio voice transmissions and electronic documents, can be obtained without physical intrusion because they are "intangible." *Olmstead*, 277 U.S. at 475 (Brandeis, J., dissenting); *see United States v. Warshak*, 631 F.3d 266, 285-86 (6th Cir. 2010) (protecting email as "the technological scion of tangible mail"). And as discussed below, digital innovations like cell site location information now enable the government to track the movements of the entire citizenry with an ease formerly unthinkable.

C. In sum, the meaning of "search" in the Founding era—as today—included seeking the whereabouts of people and their effects as well as examining documents for the information they contained. That definition plainly encompasses looking through cellular location records in order to track the movements of a person and her effects. "Whatever new methods of investigation may be devised" as technology advances, courts must "decide whether the action in question would have constituted a 'search' within the original meaning of the Fourth Amendment." *Jones*, 565 U.S. at 406 n.3. When the answer is 'yes,' "it is quite irrelevant whether there was an 18th-century analog." *Id.*

In this case, law enforcement officials obtained and examined records that revealed the location of Carpenter's cell phone over a four-month period. Pet.

App. 4a-6a. By obtaining and examining those records, they were able to identify Carpenter's whereabouts at regular, frequent intervals—showing, for instance, that he was "right where the first robbery was at the exact time of the robbery." Pet'r Br. 8 (quoting prosecutor's statement to the jury). This conduct fits squarely within the meaning of the word "search" as used in 1791. The government "look[ed] over or through" and "examine[d] by inspection" Carpenter's cell phone records "for the purpose of finding" his phone, and therefore him. Webster, *supra*. Scrutinizing those records to determine Carpenter's whereabouts was plainly an "act of seeking" and an "inquiry." Johnson, *supra*.

D. The government argues that this is a situation "when a search is not a search." *Kyllo*, 533 U.S. at 32; *see* Cert. Opp. 16 (contending that the search of Carpenter's cell phone records was not "a Fourth Amendment search"). Relying on the "third-party doctrine," the government maintains that Carpenter has "'no legitimate expectation of privacy'" in his cell phone records because they contain "'information he voluntarily turn[ed] over to third parties,'" Cert. Opp. 15 (quoting *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979)), and that the Fourth Amendment therefore sets no limits on the government's power to access and use those records. That argument rests on the definition of a "search" introduced in *Katz v. United States*, which artificially narrowed the word's meaning to violations of "an actual (subjective) expectation of privacy . . . that society is prepared to recognize as 'reasonable.'" 389 U.S. at 361 (Harlan, J., concurring).

This reliance on *Katz* denies "the people" their constitutional birthright. The *Katz* test, and its concomitant rule that "secrecy [is] a prerequisite for privacy," *Jones*, 565 U.S. at 418 (Sotomayor, J., concurring),

lacks any basis in the text and history of the Fourth Amendment. "A search is a search, even if it happens to disclose . . . . nothing of any great personal value[.]" *Arizona v. Hicks*, 480 U.S. 321, 325 (1987). Instead of continuing to probe for "understandings that are recognized and permitted by society," *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (quoting *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978)), this Court should acknowledge that searches are searches, and should focus instead—as the text commands—on guaranteeing that the right of the people to be secure against *unreasonable* searches "shall not be violated." *Cf. Ex parte Siebold*, 100 U.S. 371, 393 (1879) ("We may mystify any thing. But if we take a plain view of the words of the Constitution, and give to them a fair and obvious interpretation, we cannot fail in most cases of coming to a clear understanding of its meaning.").

The Court has inclined toward this plain-meaning approach in the past. Explaining that "warrantless visual surveillance of a home" has always been regarded as lawful, this Court has noted that the most obvious rationale for that rule does not depend on the meaning of "search." Rather, it is that "examining the portion of a house that is in plain public view, while it is a 'search' despite the absence of trespass, is not an 'unreasonable' one under the Fourth Amendment." *Kyllo*, 533 U.S. at 32 (citing *Minnesota*, 525 U.S. at 104 (Breyer, J., concurring in the judgment)). That approach, more faithful to the Amendment's text, also offers a clear path forward in an age when technology and the public's knowledge and expectations regarding that technology are constantly "in flux." *Jones*, 565 U.S. at 427 (Alito, J., concurring in the judgment).

By acknowledging that the government's conduct in this case was a "search," the Court can shift its focus away from a futile inquiry into how well the average

person understands cellular technology, and away from a fruitless quest to identify what "society" is prepared to consider reasonable with regard to the privacy of cell site location information. Instead, this Court can focus on the more straightforward question compelled by the text of the Fourth Amendment: Does granting law enforcement unfettered discretion to access and analyze that information threaten "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches"?

II. The Right of The People To Be Secure in Their Persons and Effects Against Unreasonable Searches Is Violated When the Government Has Unfettered Power To Track The People's Whereabouts Through Their Cell Phone Records

A. Whether a search is "unreasonable" under the Fourth Amendment depends upon how it affects the security of "the people," not merely the security of any individual person. This is evident both from the Amendment's text and from the history that gave rise to it—namely a widespread concern about the general insecurity caused by unconstrained authority to search.

At the time of the Fourth Amendment's adoption, the word "unreasonable" meant "not agreeable to reason" and "greater than is fit; immoderate." Johnson, *supra*. When used in political and legal discourse to describe government searches, the term had taken on a special meaning derived from the English legal tradition, which equated to "against the reason of the common law." Donohue, *supra*, at 1270. Because the common law, which was thought to embody natural reason, had rejected arbitrary search power under general warrants, *see, e.g.*, 2 Matthew Hale, *Pleas of the Crown* 150 (1736) ("a general warrant to search in

all suspected places is not good"), the power to conduct general searches was "against reason," or "unreasonable." *See* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich. L. Rev. 547, 555 n.5 (1999) (explaining how John Adams, the principal architect of the Fourth Amendment, was influenced by James Otis's condemnation of writs of assistance as "against reason," a phrase that was "often converted to 'unreasonable' [in] legal and political writings of the time"); *see also* Donohue, *supra*, at 1269-76.

"Unreasonable searches" would therefore have been understood as those that shared the flaws of searches conducted under general warrants—searches not justified by good and sufficient reasons, that went further than those reasons called for, or that were initiated without any process of disciplined reason-giving. *See* Gray, *supra*, at 160-65. That these were the hallmarks of "unreasonable searches" is further illustrated by the Fourth Amendment's Warrant Clause, which indicates that "reasonable" searches are characterized by a good and sufficient justification ("probable cause"), a process of *ex ante* reason-giving before a neutral arbiter ("Oath or affirmation"), and limited discretion (particularity).

Moreover, although the Fourth Amendment confers an individual right to be vindicated by those who themselves are subject to unlawful practices, *Rakas*, 439 U.S. at 133-34, the "unreasonable searches" from which the Amendment protects the individual are those that violate "[t]he right of *the people* to be secure in their persons, houses, papers, and effects." U.S. Const. amend. IV (emphasis added). By protecting the security of "the people" against unreasonable searches, the Framers made use of "a term of art employed in select parts of the Constitution" that "refers to a class

of persons who are part of a national community." *Verdugo-Urquidez*, 494 U.S. at 265; *see id.* at 265-66 (contrasting the term "the people" with "the words 'person' and 'accused' used in the Fifth and Sixth Amendments regulating procedure in criminal cases"); *District of Columbia v. Heller*, 554 U.S. 570, 580 (2008) (explaining that where "the people" is used in the Constitution, "the term unambiguously refers to all members of the political community, not an unspecified subset"). *Compare* Johnson, *supra* (defining "person" as an "individual or particular man or woman"), *with id.* (defining "people" as "a nation; those who compose a community").

The Framers' choice to guarantee a "right of the people" was a conscious one. They borrowed this phrase from the 1776 state constitution of Pennsylvania, which declared that "the people have a right to hold themselves, their houses, papers, and possessions free from search and seizure." Penn. Const. art. X (1776); *see* Davies, *supra*, at 677-78. By contrast, the influential Massachusetts state constitution protected the rights of "[e]very subject" against unreasonable searches and seizures. Mass. Const. pt. 1, art. XIV (1780). Although the Massachusetts provision, which flowed from the pen of John Adams, was in other respects the primary model for the Fourth Amendment, *see* Davies, *supra*, at 678, the Framers notably departed from Adams's approach by protecting "the right of the people."

This formulation spoke more directly to "the purpose of the Fourth Amendment," which "was to protect the people of the United States against arbitrary action by their own Government." *Verdugo-Urquidez*, 494 U.S. at 266; *see Jones*, 565 U.S. at 416-17 (Sotomayor, J., concurring) (referencing "the Fourth Amendment's goal to curb arbitrary exercises of police

power . . . and prevent 'a too permeating police surveillance'" (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948))). Advancing that purpose, the Amendment guards against the corroding effect on the liberty of the people as a whole that would occur if the state wielded unlimited, discretionary power to search and seize. *See Brinegar v. United States*, 338 U.S. 160, 180-81 (1949) (Jackson, J., dissenting) ("Uncontrolled search and seizure is one of the first and most effective weapons in the arsenal of every arbitrary government. . . . So a search against Brinegar's car must be regarded as a search of the car of Everyman."). "The Fourth Amendment thus gives concrete expression to a right of the people which 'is basic to a free society.'" *Camara v. Mun. Ct.*, 387 U.S. 523, 528 (1967) (quoting *Wolf v. Colorado*, 338 U.S. 25, 27 (1949)).

The reasonableness of a search must be assessed, therefore, not only with regard to the impact it has on the privacy or property of the individual searched in that case. Consideration must also be given, as the text of the Fourth Amendment indicates, to whether allowing the government to conduct that type of search would violate the security of "the people." *See* Luke M. Milligan, *The Forgotten Right To Be Secure*, 65 Hastings L.J. 713, 738-50 (2014) (explaining that the Fourth Amendment confers on the people a right to be "free from fear" of unreasonable searches). Therefore, the question is whether the decision to engage in a type of search can be left to the unfettered discretion of government agents, free of "oversight from a coordinate branch," *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring), without compromising the security of the people as a whole.

Historical context buttresses this textual inference. Given the heritage of general warrants and

writs of assistance, the Founders feared giving the federal government "free rein to search for potential evidence of criminal wrongdoing." Donohue, *supra*, at 1194. Such broad discretion was intolerable to the Founders precisely because of its oppressive impact on the political community, or "the people," as a whole. *See* Gray, *supra*, at 146-56.

In *Wilkes v. Wood*, for instance, the court condemned the unbounded discretion that general warrants conferred on the officers who executed them. Because general warrants did not require agents to identify particular suspects or to inventory items to be seized, "a discretionary power [was] given to messengers to search wherever their suspicions may chance to fall." 98 Eng. Rep. at 498. In *Money v. Leach*, another of the general warrant cases, the court similarly declared, "It is not fit, that the receiving or judging of the information should be left to the discretion of the officer." 97 Eng. Rep. 1075, 1088 (1765).

Though few people actually were victims of searches conducted pursuant to general warrants, these courts emphasized that the mere existence of such warrants made the entire nation vulnerable to them—depriving the people of security against arbitrary and unreasonable searches. As explained in *Wilkes*, the establishment of general search power "may affect the person and property of every man in this kingdom, and is totally subversive of the liberty of the subject." 98 Eng. Rep. at 498. In *Entick v. Carrington*, the court likewise warned that if general warrants were permitted, "no subject whatsoever is privileged from this search . . . . the secret cabinets and bureaus of every subject in this kingdom will be thrown open to the search and inspection of a messenger . . . .

and every house will fall under the power of a secretary of state to be rummaged before proper conviction." 19 How. St. Tr. at 1063, 1071.

In the eighteenth century, therefore, arbitrary and unfettered power to search was viewed as endangering the nation itself. This existential threat, rather than the damage suffered by any individual person, was described as the motivating force behind the verdict of the jury in *Huckle v. Money*: "[T]he small injury done to the plaintiff, or the inconsiderableness of his station and rank in life did not appear to the jury in that striking light in which the great point of law touching the liberty of the subject appeared to them at the trial; they saw a magistrate over all the King's subjects, exercising arbitrary power, violating Magna Charta, and attempting to destroy the liberty of the kingdom[.]" 95 Eng. Rep. 768, 769 (1763). This general search power was all the more perilous because it was traditionally "used to stifle religious and political dissent." Milligan, *supra*, at 749; *see* Cuddihy, *supra*, at 122-23; Donohue, *supra*, at 1208-10.

Challenges to writs of assistance in the American colonies highlighted the same theme: discretionary search authority raised the specter of subjugation to arbitrary power for every citizen, imperiling the political body as whole. "In 1761, the patriot James Otis delivered a speech in Boston denouncing the use of writs of assistance" in *Paxton's Case*. *Riley*, 134 S. Ct. at 2494. Otis declared that the writ being sought was "a power that places the liberty of every man in the hands of every petty officer," representing "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law." Otis, *supra*. Because the writ "is directed to every subject in the King's dominions," Otis declared,

"[e]very one with this writ may be a tyrant . . . . accountable to no person for his doings. Every man may reign secure in his petty tyranny." *Id.* According to a young John Adams, who witnessed the fiery argument, "Otis's speech was 'the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born.'" *Riley*, 134 S. Ct. at 2494 (citations omitted).

Otis drew special attention to the danger of discretionary search power in singling out targets based on personal animus or other improper motives. As he put it, "Every man prompted by revenge, ill humor, or wantonness, to inspect the inside of his neighbor's house, may get a Writ of Assistance." Otis, *supra*. To show that the "wanton exercise of this power" was "not a chimerical suggestion of a heated brain," Otis related an incident in which an officer, called to task by a judge and a constable for "breach of the Sabbath-day Acts," retaliated against both by ordering the searches of their houses, "from the garret to the cellar," for "uncustomed goods." *Id.* A later commentator similarly warned that "if magistrates had a power of arresting men . . . merely upon their own suspicions, or pretended suspicions, they might cause any person how innocent soever, to be thrown into prison whenever they thought fit." 2 Francis Maseres, *The Canadian Freeholder: In Three Dialogues Between an Englishman and a Frenchman* 246 (1779).

Early decisions in American courts likewise emphasized that the security of the people would be compromised if government officers were given broad, discretionary search powers. *See Frisbie v. Butler*, 1 Kirby 213, 215 (Conn. Super. Ct. 1787) (finding "clearly illegal" a general warrant to search all places that "the complainant should suspect"). Placing such

arbitrary power in the hands of state agents threatened the security of the entire community. *See Grumon v. Raymond*, 1 Conn. 40, 43 (1814) (declaring unlawful "a warrant to search all suspected places" for stolen goods, because "every citizen of the United States within the jurisdiction of the justice to try for theft, was liable to be arrested"). That threat was heightened because unbounded, discretionary search power inevitably invited abuse. *See id.* at 44 ("It would open a door for the gratification of the most malignant passions, if such process issued by a magistrate should skreen [an officer] from damages."); *Bell v. Clapp*, 10 Johns. 263, 266 (N.Y. Sup. Ct. 1813) (explaining that the constitutional checks imposed on the operation of search warrants arose from "a strong jealousy of the abuses incident to them").

Considering the impact on the security of "the people" as a whole if the government were given unfettered power to search is not only faithful to the Amendment's text and history, it is also capable of ensuring that Fourth Amendment rights are not left "at the mercy of advancing technology." *Kyllo*, 533 U.S. at 35. The digital tools employed by government agents today have gone far beyond "augmenting the sensory faculties bestowed upon them at birth," *Knotts*, 460 U.S. at 282, and increasingly exploit the fact that "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks," *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). Modern technology, "by making available at a relatively low cost . . . a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track," *id.* at 416, has fundamentally changed the state's capacity to monitor the activities of the people. That develop-

ment, if left unchecked, will "alter the relationship between citizen and government in a way that is inimical to democratic society." *Id.* The Fourth Amendment is directed against this threat and demands checks sufficient to guarantee that "the right of the people to be secure . . . shall not be violated."

B. Protecting the security of "the people" against unreasonable searches requires considering more than simply the *type* of information gathered in a search, and whether it has been "knowingly expose[d] to the public," *Katz*, 389 U.S. at 351, or "third parties," *Smith*, 442 U.S. at 744. Consideration must also be given to the *means* by which the government gathers the information and the overall effect on the security of "the people" if government agents were to enjoy unfettered discretion to employ those means. *See* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 Minn. L. Rev. 62, 101-02 (2013).

To illustrate, consider the difference between human surveillance and modern tracking technologies. It may be perfectly reasonable under the Fourth Amendment to leave decisions to conduct human surveillance to the unfettered discretion of law enforcement. That is because human surveillance is inherently limited in scope (officers can be in only one place at a time), difficult to conduct on a broad scale (there are only so many police officers), and thus relatively costly in time and money. *See* Gray & Citron, *supra*, at 124-25. These features of human surveillance mean that it is seldom used on a grand scale or for extended periods of time, and even then only for compelling reasons. *Jones*, 565 U.S. at 429 (Alito, J., concurring in the judgment). That, in turn, means that leaving the decision to conduct human surveillance to the unfettered discretion of government agents is unlikely to

threaten "the right of the people to be secure . . . against unreasonable searches and seizures."

By contrast, consider technologies such as global positioning system ("GPS") and radio-frequency identification ("RFID") monitoring. Tracking programs that use these technologies have extraordinary capacity in terms of scope, because GPS and RFID chips are commonly embedded in personal electronic devices, computers, cars, driver's licenses, passports, credit cards, and even clothes. *See*, Gray, *supra* at 23-30. These programs are also highly scalable, because they can be automated and monitored by computers, and are increasingly inexpensive as well. *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *id.* at 429 (Alito, J., concurring in the judgment). Together, these features make granting government agents unfettered access to GPS or RFID technologies a pernicious threat to the security of the people against unreasonable searches, because those technologies can easily facilitate programs of broad and indiscriminate surveillance, condemning each of us to live in fear that we could be surveilled at any time or all the time.

This Court has acknowledged that the distinction illustrated by this example might make a difference under the Fourth Amendment. In *Knotts*, the Court held that it was constitutionally permissible for narcotics officers to visually track the public movements of a suspect without a warrant, even when those efforts were aided by a relatively primitive radio beeper device. *Knotts*, 460 U.S. at 277, 285. In doing so, however, the Court emphasized "the limited use which the government made of the signals" from the beeper, and that the technology merely enhanced the "efficiency" of what was still a resource-intensive effort to track a particular suspect's vehicle during a single journey. *Id.* at 278 (noting that the pursuing officers "lost the

signal from the beeper" at one point and were forced to call upon "the assistance of a monitoring device located in a helicopter").

As the *Knotts* Court explained, the limitations of the beeper technology used there meant that granting officers unfettered access did not raise any danger of "'twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision.'" *Id.* at 283-84 (quoting respondent's brief). Presciently, the Court promised that "if such dragnet-type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." *Id.* at 284; *see Jones*, 565 U.S. at 412 (suggesting that while continuous visual observation of a suspect's movements over a four-week period is constitutionally permissible, "[i]t may be that achieving the same result through electronic means . . . is an unconstitutional invasion of privacy").

The threat of dragnet surveillance that was mere speculation in *Knotts* is reality today. Electronic devices that are increasingly essential to modern life now generate, as a matter of course, a perpetual record of a person's movements, "mak[ing] long-term monitoring relatively easy and cheap." *Jones*, 565 U.S. at 429 (Alito, J., concurring in the judgment). What is more, the government is often spared the burden of conducting the monitoring itself because it can simply reap the fruits of routine data gathering by third parties. As a result, the state's ability to track its citizens is no longer constrained by the need to single out particular suspects in advance, or to invest the time and resources that prolonged surveillance demands.

These considerations reveal why it is not "incongruous" to impose constitutional constraints on the use

of GPS technology to monitor a car's movements, "for even a brief time," while allowing the police broader discretion to "follow the same car for a much longer period using unmarked cars and aerial assistance." *Id.* at 425 (Alito, J., concurring in the judgment). The need to devote significant time and resources to any long-term surveillance is precisely why the people can be secure in their persons and effects against the danger that police will track their movements using traditional methods without good reason to do so. *See id.* at 429 ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken."). By contrast, GPS technology enables the police to generate "a precise, comprehensive record" of a car's movements with little effort. *Id.* at 415 (Sotomayor, J., concurring). The disparity becomes even greater when police can obtain that comprehensive record from third-party commercial entities well after the events in question have taken place. Such is the case with cell site location information.

Modern cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley*, 134 S. Ct. at 2484; *cf. City of Ontario v. Quon*, 560 U.S. 746, 760 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."). By 2014, "nearly three-quarters of smart phone users report[ed] being within five feet of their phones most of the time." *Riley*, 134 S. Ct. at 2490.

As the government acknowledges, "a cell-phone user *must* reveal his general location to a cell tower in order for the cellular service provider to connect a call." Cert. Opp. 15 (emphasis added). Anyone who uses this essential tool of modern life has no choice but to accept the creation of a continuous digital trail of her locations and movements. Perversely, the government argues that this inevitability is why the Fourth Amendment should place no limits on the government's acquisition of that digital trail. *See id.* at 16 (citing *Smith*, 442 U.S. at 745). That position, which permits "technology to erode the privacy guaranteed by the Fourth Amendment," *Kyllo*, 533 U.S. at 34, is utterly backwards if one is concerned about safeguarding the security of the people against the unreasonable and arbitrary use of state power.

When Fourth Amendment analysis focuses on the *method* employed by the government and its potential effects on the security of the people—not just on the information obtained—it becomes clear why certain high-tech means of conducting searches must be subject to constitutional regulation even though searches for the same information using traditional means are not. Government officers can follow people from place to place in search of information about their activities and whereabouts without threatening the security of the people because practical obstacles make it difficult to use this method in excess. But the rise of modern cell phones, "based on technology nearly inconceivable just a few decades ago," *Riley*, 134 S. Ct. at 2484, has given the government ready means to conduct "twenty-four hour surveillance of any citizen of this country." *Knotts*, 460 U.S. at 283. Unfettered government access to these technologies, being inimical to "a society which chooses to dwell in reasonable security and freedom from surveillance,"

Johnson, 333 U.S. at 14, is constitutionally unreasonable. "The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment." *Kyllo*, 533 U.S. at [illegible] n.2.

Limitless access to location data is all the more unreasonable because of its potential to reveal "political and religious beliefs, sexual habits, and so on." *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring). "Awareness that the Government may be watching chills associational and expressive freedoms," and "the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse." *Id.* These concerns echo those of the Founding generation, which had learned that discretionary search power, when lodged in the state, is apt to be directed against disfavored ideas. *See supra* at 19.

C. The "imprecise nature" of cell site location information, Cert. Opp. 25, does not ameliorate the problems discussed above. Even when the technology used in a particular case is "relatively crude," the rules this Court adopts "must take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U.S. at 35-36. The precision of cellular location data is improving every day. *See* Pet'r Br. 27-29. And in any event, the technology used in this case proved fully capable of establishing Carpenter's proximity to particular places at particular times. *See* Pet. App. 6a.

More problematic still is that the government, in asking this Court to distinguish between GPS data and the location records used here, introduces "vexing" line-drawing problems akin to those that worried the Court in *Jones*. 565 U.S. at 412-13. The government does not explain how precise is *too* precise, and indeed

As the government acknowledges, "a cell-phone user *must* reveal his general location to a cell tower in order for the cellular service provider to connect a call." Cert. Opp. 15 (emphasis added). Anyone who uses this essential tool of modern life has no choice but to accept the creation of a continuous digital trail of her locations and movements. Perversely, the government argues that this inevitability is why the Fourth Amendment should place no limits on the government's acquisition of that digital trail. *See id.* at 16 (citing *Smith*, 442 U.S. at 745). That position, which permits "technology to erode the privacy guaranteed by the Fourth Amendment," *Kyllo*, 533 U.S. at 34, is utterly backwards if one is concerned about safeguarding the security of the people against the unreasonable and arbitrary use of state power.

When Fourth Amendment analysis focuses on the *method* employed by the government and its potential effects on the security of the people—not just on the information obtained—it becomes clear why certain high-tech means of conducting searches must be subject to constitutional regulation even though searches for the same information using traditional means are not. Government officers can follow people from place to place in search of information about their activities and whereabouts without threatening the security of the people because practical obstacles make it difficult to use this method in excess. But the rise of modern cell phones, "based on technology nearly inconceivable just a few decades ago," *Riley*, 134 S. Ct. at 2484, has given the government ready means to conduct "twenty-four hour surveillance of any citizen of this country." *Knotts*, 460 U.S. at 283. Unfettered government access to these technologies, being inimical to "a society which chooses to dwell in reasonable security and freedom from surveillance,"

Johnson, 333 U.S. at 14, is constitutionally unreasonable. "The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment." *Kyllo*, 533 U.S. at 35 n.2.

Limitless access to location data is all the more unreasonable because of its potential to reveal "political and religious beliefs, sexual habits, and so on." *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring). "Awareness that the Government may be watching chills associational and expressive freedoms," and "the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse." *Id.* These concerns echo those of the Founding generation, which had learned that discretionary search power, when lodged in the state, is apt to be directed against disfavored ideas. *See supra* at 19.

C. The "imprecise nature" of cell site location information, Cert. Opp. 25, does not ameliorate the problems discussed above. Even when the technology used in a particular case is "relatively crude," the rules this Court adopts "must take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U.S. at 35-36. The precision of cellular location data is improving every day. *See* Pet'r Br. 27-29. And in any event, the technology used in this case proved fully capable of establishing Carpenter's proximity to particular places at particular times. *See* Pet. App. 6a.

More problematic still is that the government, in asking this Court to distinguish between GPS data and the location records used here, introduces "vexing" line-drawing problems akin to those that worried the Court in *Jones*. 565 U.S. at 412-13. The government does not explain how precise is *too* precise, and indeed

"offers no practical guidance for the application of this standard." *Kyllo*, 533 U.S. at 39. To the extent the government suggests that this Court rely on such distinctions to defer consideration of the weighty questions raised by digital location tracking, the government merely asks the Court to perpetuate uncertainty, thereby leaving the people insecure against the threat of unreasonable searches posed by these technologies.

III. The Stored Communications Act's Protections Are Inadequate

The Fourth Amendment sets out an imperative: the right of the people to be secure against unreasonable searches "shall not be violated." To meet that command, the Amendment compels the imposition of limits on the government's ability to deploy certain types of searches. The prime example of such a constraint is found in the Amendment itself, which specifies that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

By requiring probable cause—sworn to by oath or affirmation, and evaluated by a neutral magistrate—along with particularity regarding the place to be searched, the Warrant Clause "prevents the issue of warrants on loose, vague or doubtful bases of fact," promoting the Amendment's "purpose to protect against all general searches," which are inherently "obnoxious to fundamental principles of liberty." *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 357 (1931); *see Davies*, *supra*, at 576-77 (the Amendment "did not simply seek to provide a post-intrusion remedy," but rather "adopted a preventive strategy . . . prohibiting even the issuance of a too-loose warrant");

Milligan, *supra*, at 746-50 (criticism of general warrants focused less on their execution and more on their "issuance," "existence," and "power"). Together, these safeguards protect the people from being "secure only in the discretion of police officers . . . engaged in the often competitive enterprise of ferreting out crime." *Coolidge v. New Hampshire*, 403 U.S. 443, 449 (1971) (quoting *Johnson*, 333 U.S. at 14).

Similar protections are needed here, given the serious threat that government access to cell site location information poses to the security of the people. *See supra* at 24-27. Although the SCA includes requirements that in some ways resemble those of the Warrant Clause, its protections fall short given the formidable power of location data as a tool for monitoring the activities of the people.

The SCA permits the government to obtain cell site location information if it offers "specific and articulable facts showing that there are reasonable grounds to believe" that the records "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). It does not require the government to limit the records sought, beyond the general requirement of relevance to an investigation, or to demonstrate probable cause, or to provide a sworn statement affirming the facts set forth in the government's application.

These standards fail to impose sufficient constraints on the use of cell site location information to conduct searches. Mere relevance to an investigation does not adequately constrain the scope of the data the government can obtain under the SCA, either in quantity or in duration. That is especially true because of the potential usefulness, or at least perceived usefulness, of exploiting such data in a dragnet-like search for information about potential suspects. *See* Cert. Opp. 25 (arguing that cell site location information is

"particularly valuable during the early stages of an investigation, when the police [may] lack probable cause and are confronted with multiple suspects" (quoting *United States v. Davis*, 785 F.3d 498, 518 (11th Cir. 2015))). For example, the loose relevance standard of the SCA could permit widespread surveillance of all cell phones in a "high crime" area where the government is investigating a rash of ongoing offenses.

Indeed, under a similar legal standard—requiring "a statement of facts showing that there are reasonable grounds to believe that the [records] sought are relevant to an authorized investigation," 50 U.S.C. § 1861(b)(2)(B), multiple federal district court judges over a period of years approved the indiscriminate nationwide collection of calling records because, the government asserted, bulk analysis of such records could reveal "connections between known and unknown international terrorist operatives." *In re F.B.I. App. for an Order Requiring Prod. of Tangible Things*, No. BR 13-109, 2013 WL 5741573, at *6 (FISA Ct. Aug. 29, 2013); *accord ACLU v. Clapper*, 959 F. Supp. 2d 724, 746 (S.D.N.Y. 2013) (rejecting argument that the collection "is too broad and contains too much irrelevant information" to meet the statutory standard, "[b]ecause without all the data points, the Government cannot be certain it connected the pertinent ones"), *aff'd in part, vacated in part, remanded*, 785 F.3d 787 (2d Cir. 2015). Regardless of whether those rulings were correct in the context of the surveillance program at issue, they reveal the elasticity of a standard that requires only relevance to an investigation.

Even on the facts of this case, the overbreadth of collection that the SCA permits is apparent. The government suspected Carpenter of involvement in a number of store robberies. Pet. App. 3a. But rather than limiting its request "to only the days on which the

robberies occurred," the government sought—and the court approved—the acquisition of records showing his locations and movements over five months (152 days), which ultimately yielded more than four months' worth of data (127 days). Pet. 4-5 & n.2; *see* Pet. App. 52a. The records were used in court, however, only to establish that Carpenter was near the sites of four robberies. Pet. App. 6a.

Moreover, by the time the government requested Carpenter's records, it seems already to have had probable cause to arrest him and seek his cell phone records for the specific times of the robberies. *See* Pet. App. 3a (explaining that a fellow suspect had confessed and given information about his accomplices and their telephone numbers); *cf.* Pet. App. 5a (indicating that ultimately seven of Carpenter's associates testified against him at trial); Cert. Opp. 6 ("The government also introduced videotapes and eyewitness testimony placing petitioner near the relevant robbery scenes."). Given this, it would not have unduly burdened the government to obtain a traditional warrant for Carpenter's cell phone records, as the SCA also permits. *See* 18 U.S.C. § 2703(c)(1)(A); *cf. Riley*, 134 S. Ct. at 2493 ("Recent technological advances" have "made the process of obtaining a warrant itself more efficient."). By helping prevent unnecessarily broad data requests, and by ensuring that all requests are justified by facts independently evaluated by a magistrate under a standard of probable cause, such a requirement would "have the salutary effect of ensuring that use of [location data] is not abused," *Karo*, 468 U.S. at 717, thereby guaranteeing the security of the people against unreasonable searches conducted using cell site location information.

CONCLUSION

For the foregoing reasons, the judgment of the Sixth Circuit Court of Appeals should be reversed.

Respectfully submitted,

ELIZABETH B. WYDRA
BRIANNE J. GOROD*
BRIAN R. FRAZELLE
CONSTITUTIONAL
ACCOUNTABILITY CENTER
1200 18th Street NW, Suite 501
Washington, D.C. 20036
(202) 296-6889
brianne@theusconstitution.org

Counsel for Amici Curiae

August 14, 2017 * Counsel of Record

RECORD AND BRIEFS

No. 16-402

Supreme Court, U.S.
FILED
AUG 14 2017
OFFICE OF THE CLERK

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

BRIEF FOR TECHNOLOGY COMPANIES AS AMICI CURIAE IN SUPPORT OF NEITHER PARTY

SETH P. WAXMAN
Counsel of Record
JONATHAN G. CEDARBAUM
CATHERINE M.A. CARROLL
ROBBIE MANHAS
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Ave., NW
Washington, DC 20006
(202) 663-6000
seth.waxman@wilmerhale.com

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES iii

STATEMENT OF INTEREST 1

SUMMARY OF ARGUMENT 9

ARGUMENT 12

I. FOURTH AMENDMENT DOCTRINE MUST ADAPT TO THE CHANGING REALITIES OF THE DIGITAL ERA 12

A. Digital Data And Devices Are Pervasive, Personal, And Often Necessary To Modern Life 14

B. Users Of Digital Technologies Cannot Avoid Transmitting Sensitive Data To Service Providers, But They Expect That Data To Remain Private 17

C. Amici's Compliance With Law-Enforcement Requests Respects User Privacy 21

II. RIGID ANALOG-ERA RULES SHOULD YIELD TO CONSIDERATION OF REASONABLE EXPECTATIONS OF PRIVACY IN THE DIGITAL AGE 23

A. A Flexible Test Grounded In Today's Reasonable Expectations Of Privacy Should Govern In The Digital Context 23

B. Transmission To A Service Provider Should Not Automatically Foreclose Protection Of Digital Data 26

TABLE OF CONTENTS—Continued

Page

C. "Non-Content" Digital Data Should Not Automatically Be Excluded From Protection 29

CONCLUSION 32

TABLE OF AUTHORITIES

CASES

Page(s)

Ex parte Jackson, 96 U.S. 727 (1878) 29, 30

In re Google Inc. Cookie Placement Consumer Privacy Litigation, 806 F.3d 125 (3d Cir. 2015) 32

Katz v. *United States*, 389 U.S. 347 (1967) 24

Kyllo v. *United States*, 533 U.S. 27 (2001) 12, 25, 28

Missouri v. *McNeely*, 133 S. Ct. 1552 (2013) 21

NAACP v. *Alabama*, 357 U.S. 449 (1958) 32

Oliver v. *United States*, 466 U.S. 170 (1984) 23

Packingham v. *North Carolina*, 137 S. Ct. 1730 (2017) 12, 15, 17, 26

Riley v. *California*, 134 S. Ct. 2473 (2014) ..... *passim*

Smith v. *Maryland*, 442 U.S. 735 (1979) 12, 26, 27, 28

State v. *Zeller*, 172 Wash. App. 1008 (2012) 21

United States v. *Dotson*, 715 F.3d 576 (6th Cir. 2013) 17

United States v. *Figueroa*, 2008 WL 5423982 (E.D. Wis. Dec. 30, 2008) 14

United States v. *Holm*, 326 F.3d 872 (7th Cir. 2003) 17

United States v. *Jones*, 565 U.S. 400 (2012) 18, 24, 25, 27, 30

TABLE OF AUTHORITIES—Continued

Page(s)

United States v. *Karo*, 468 U.S. 705 (1984) 25, 28

United States v. *LaCoste*, 821 F.3d 1187 (9th Cir. 2016) 14, 17

United States v. *Miller*, 425 U.S. 435 (1976) 12, 26

United States v. *Peterson*, 248 F.3d 79 (2d Cir. 2001) 25

United States v. *Pineda-Moreno*, 617 F.3d 1120 (9th Cir. 2010) 31

United States v. *Sofsky*, 287 F.3d 122 (2d Cir. 2002) 14

United States v. *Voelker*, 489 F.3d 139 (3d Cir. 2007) 25

United States v. *Warshak*, 631 F.3d 266 (6th Cir. 2010) 21, 23, 29, 30

DOCKETED CASES

Microsoft v. *United States*, No. 16-cv-00538 (W.D. Wash.) 22

STATUTES, RULES AND LEGISLATIVE MATERIALS

Stored Communications Act, 18 U.S.C. § 2703 ..... 21, 30

Fed. R. Crim. P. 4.1 21

H.R. Rep. No. 114-528 (2016) 21

TABLE OF AUTHORITIES—Continued

Page(s)

OTHER AUTHORITIES

Anderson, Monica, *6 Facts About Americans and their Smartphones*, Pew Res. Ctr., Apr. 1, 2015, http://www.pewresearch.org/fact-tank/2015/04/01/6-facts-about-americans-and-their-smartphones/ 14

Apple Inc., *Legal Process Guidelines: Government & Law Enforcement Within the United States*, https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf (visited Aug. 13, 2017) 22

Apple Inc., *Privacy Policy*, https://www.apple.com/legal/privacy/en-ww/ (visited Aug. 14, 2017) 20

Apple Inc., *Report on Government and Private Party Requests for Customer Information*, https://images.apple.com/legal/privacy/transparency/requests-2016-H2-en.pdf (visited Aug. 13, 2017) 22

Bellovin, Steven M. et al., *It's Too Complicated: How the Internet Upends* Katz, Smith, *and Electronic Surveillance Law*, 30 Harv. J.L. & Tech. 1 (2016) 17, 18

Bowman, Courtney M., *A Way Forward After* Warshak: *Fourth Amendment Protections for E-mail*, 27 Berkeley Tech. L.J. 809 (2012) 15

TABLE OF AUTHORITIES—Continued

Page(s)

CTIA, *Semi-Annual Wireless Industry Survey* (2011), http://files.ctia.org/pdf/CTIA_Survey_MY_2011_Graphics.pdf (visited Aug. 14, 2017) 13

Crist, Ry, *Home Automation Buying Guide*, CNet (Apr. 28, 2017 9:07 a.m.), https://www.cnet.com/news/smart-home-buying-guide-home-automation/ 16

Colb, Sherry F., *What Is A Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of A Remedy*, 55 Stan. L. Rev. 119 (2002) 29

Dewey, Caitlin, *How Many Hours of Your Life Have You Wasted on Work Email? Try our Depressing Calculator*, Wash. Post, Oct. 3, 2016, https://www.washingtonpost.com/news/the-intersect/wp/2016/10/03/how-many-hours-of-your-life-have-you-wasted-on-work-email-try-our-depressing-calculator/?utm_term=.54666f34830d 14

Dropbox, Inc., *Privacy Policy*, https://www.dropbox.com/privacy (visited Aug. 14, 2017) 20

Dropbox, Inc., *Transparency Overview*, https://www.dropbox.com/transparency (visited Aug. 13, 2017) 22

TABLE OF AUTHORITIES—Continued

Page(s)

Facebook, Inc., *Two Billion People Coming Together on Facebook* (June 27, 2017), https://newsroom.fb.com/news/2017/06/two-billion-people-coming-together-on-facebook/ 15

Google Inc., *Cloud Platform Security*, https://cloud.google.com/security/compliance (visited Aug. 13, 2017) 20

Google Inc., *Privacy, Your Security Comes First in Everything We Do*, https://privacy.google.com/your-security.html (visited Aug. 13, 2017) 20

Madden, Mary & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Research Center, May 20, 2015, http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ 19

Madden, Mary, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Center (Nov. 14, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ 18

Marya, Radhika, *Cellphones are now essentials for the poor*, USA Today, Sept. 14, 2013, https://www.usatoday.com/story/money/personalfinance/2013/09/14/cellphones-for-poor-people/2805735/ 14

TABLE OF AUTHORITIES—Continued

Page(s)

Mastroianni, Brian, *Survey: More Americans Worried About Data Privacy than Income*, CBS News, Jan. 28, 2016, http://www.cbsnews.com/news/truste-survey-more-americans-concerned-about-data-privacy-than-losing-income/ 19

Meeker, Mary, *2016 Internet Trends Report*, Kleiner Perkins Caufield & Byers (June 1, 2016), http://www.kpcb.com/blog/2016-internet-trends-report 15

Microsoft Trust Center, *Security, Audits, and Certifications*, https://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Security_Audit.htm (visited Aug. 13, 2017) 20

National Security Telecommunications Advisory Committee, *NSTAC Report to the President on Emerging Technologies: Strategic Vision Executive Summary* (May 18, 2017), https://www.dhs.gov/sites/default/files/publications/Draft%20NSTAC%20ETSV%20Report%20Executive%20Summary%20508%20Compliant_1.pdf 16

Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 Harv. L. Rev. 1924 (2017) 16, 27

TABLE OF AUTHORITIES—Continued

Page(s)

Organisation for Economic Co-operation Development, *Bridging the Digital Divide*, https://www.oecd.org/site/schoolingfortomorrowknowledgebase/themes/ict/bridgingthedigitaldivide.htm (visited Aug. 13, 2017) 13

Parlante, Nick, *The Internet-TCP/IP, CS101—Introduction to Computing Principles*, CS01, https://web.stanford.edu/class/cs101/network-3-internet.html (visited Aug. 13, 2017) 17

Pesciotta, Daniel T., *I'm Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st Century*, 63 Case W. Res. L. Rev. 187 (2012) 28

Pew Research Center, *Mobile Fact Sheet* (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/ 13

Pew Research Center, *Online Shopping and E-Commerce* (Dec. 19, 2016), http://www.pewinternet.org/2016/12/19/online-shopping-and-e-commerce/ 15

Radicati Group, Inc., *Email Statistic Report, 2017-2021* (Feb. 6, 2017), http://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf. 13

Shuler, Rus, *How Does The Internet Work?* (2002), https://www.scribd.com/document/316562293/Rus-Shuler-How-Does-the-Internet-Work 17

TABLE OF AUTHORITIES—Continued

Page(s)

Silliman, Craig, *Musing About the Third Party Doctrine During Network Planning Meetings* (Oct. 10, 2016), https://www.linkedin.com/pulse/musing-third-party-doctrine-during-network-planning-craig-silliman 31

Snap Inc., *Transparency Report*, https://www.snap.com/en-US/privacy/transparency/2015-02-28 (visited Aug. 13, 2017) 22

Twitter Inc., *Transparency Report: United States*, https:// transparency. twitter.com/en/countries/us.html (visited Aug. 13, 2017) 22

United States Government Accountability Office, *Internet of Things: Communities Deploy Projects By Combining Federal Support With Other Funds And Expertise*, GAO-17-570 (July 2017) 16, 17

Warner, Timothy L., *Protect Your Online Privacy by Removing Exif Data from Your Photos*, Que Publishing (May 15, 2014), http://www.quepublishing.com/articles/article.aspx?p=2216446 16

Wasik, Bill, *In the Programmable World, All Our Objects Will Act As One*, Wired, May 14, 2013 6:30 a.m., https://www.wired.com/2013/05/internet-of-things-2/ 16

STATEMENT OF INTEREST[1]

Amici are the world's leading technology companies. Billions of people rely daily on amici's search engines, email services, social networks, smartphones, cloud storage, Internet-based devices and applications, and wireless networks for their businesses and personal lives.

Amici have a substantial interest in the legal standards governing law-enforcement access to data about their customers. Those customers entrust amici with some of their most intimate information, including what they search, where they are, and details of their daily lives. Given the sensitivity of this data, amici work continuously to secure their customers' privacy. And amici agree that Fourth Amendment doctrine should recognize that, in the evolving digital era, where such data is disclosed to or collected by service providers to provide technologies that are increasingly integrated into daily life, people reasonably expect that their data will be stored securely and remain private.

Although amici do not take a position on the outcome of this case, they believe Fourth Amendment protections for digital data should be strong. Rigid rules such as the third-party doctrine and the content/non-content distinction make little sense in the context of digital technologies and should yield to a more nuanced understanding of reasonable expectations of privacy, including consideration of the sensitivity of the data

---

[1] No counsel for a party authored this brief in whole or in part, and no entity or person other than amici and their counsel made a monetary contribution intended to fund the preparation or submission of this brief. Letters consenting to the filing of amicus briefs are on file with the Clerk.

and the circumstances under which such data is collected by or disclosed to third parties as part of people's participation in today's digital world.

Airbnb is a trusted community marketplace for people to list, discover, and book unique accommodations in more than 65,000 cities and 191 countries. Since its founding in 2008, there have been over 200 million guest arrivals in the over 4 million listings on Airbnb worldwide. While negative incidents are rare, Airbnb works with law enforcement to protect the rights of its Hosts, its Guests, and the community at large. At the same time, Airbnb respects the privacy interests of its community members. Airbnb sets forth in its law-enforcement guidelines how and when it complies with its legal obligations to provide user data to law enforcement. Airbnb publishes a Transparency Report to inform the public of the nature and volume of law-enforcement requests it receives and processes annually.

Apple Inc. offers highly secure hardware, software, and servers to customers worldwide. Apple's business strategy leverages its unique ability to design and develop its own operating systems, hardware, application software, and services to provide customers products and solutions with superior security, ease of use, seamless integration, and innovative design. In addition to the iPhone, iPad, Mac computer, and iPod, Apple offers its users iCloud—a cloud service for storing photos, contacts, calendars, documents, device backups, and more, keeping everything up to date and available to customers on whatever device they are using. Apple is committed its users' privacy and to helping users understand how it handles their personal information. Apple strives to provide straightforward

disclosures when it is compelled to comply with requests for user data from law enforcement.

Box is a cloud-based content-management platform that makes it easier for businesses to securely collaborate, share, and manage their content. Today, more than 74,000 businesses, including 64 percent of the Fortune 500, rely on Box to power how they work. Box respects the privacy rights of its users, collecting only the information necessary to authenticate the authorized user and provide access to the Box Service. Box invests significant resources in maintaining data-protection certifications to support its customers and effectuates personal data transfers from the European Union pursuant to Box's global privacy rules.

Cisco Systems, Inc. is the worldwide leader in providing infrastructure for the Internet. It also offers services including remote data centers, wireless-internet services, internet-security services, and collaboration tools, all managed from data centers operated by Cisco. Cisco is committed to protecting users' personal information. Its privacy statements reflect global principles and standards on handling personal information, including notice and user choice of data use and data security. Cisco regularly publishes information about requests for customer data that it receives from agencies around the world. Cisco believes law-enforcement and national-security agencies should go directly to its customers to obtain information or data regarding those entities, their employees, and users.

Dropbox, Inc. provides file-storage, synchronization, and collaboration services to customers and businesses worldwide. Its services empower people to work the way they want, on any device, wherever they go. Users entrust Dropbox with their most important

files, including documents and photos. When users put their files in Dropbox, they can rest assured that their data is secure and their own. Dropbox has a specialized privacy team dedicated to ensuring that privacy protections are built into Dropbox's products and services from the ground up. Dropbox's Government Request Principles reflect its commitment to protecting user privacy when responding to government requests for user data. Dropbox also publishes regular transparency reports about law-enforcement requests.

Evernote Corporation builds technology that enables individuals and teams to capture, organize, find, and share ideas in any form, on any Internet-connected device, forever. The Evernote app is available across platforms on desktop, mobile, or on the web. Users can input, upload, or store text, images, and other data. Evernote has more than 200 million consumer and business users in the United States and around the world. Evernote collects subscriber information, log data, location information, and device information and is committed to the privacy and security of its users' data. Evernote's Privacy Center and Privacy Policy inform users about the data Evernote collects and uses; Evernote's Security Overview describes how Evernote protect users' data. Evernote's Transparency Report reflects the volume of third-party demands Evernote receives for disclosure of user data. Evernote describes its user-notice policy and other practices for responding to such demands on its Information for Authorities website.

Facebook, Inc. provides a free Internet-based social-media service that gives more than two billion people the power to build communities and bring the world closer together. People use Facebook to stay connected with friends and family, to build communities, to

discover what is going on in the world, and to express what matters to them. People provide their names, phone numbers, and/or e-mail addresses when signing up for Facebook. As set forth in its Data Policy, Facebook also collects other information to provide its service, such as IP addresses and device-location data. Facebook is committed to protecting the privacy of the people who use its services. Facebook has robust privacy settings that allow people to control the audience of the information they choose to share. Facebook has also developed a privacy check-up tool to ensure that people's privacy settings reflect their desired level of privacy. Facebook closely reviews all requests for data from law enforcement and notifies people of requests for their information before disclosure unless prohibited by law from doing so or in exceptional circumstances. Facebook regularly produces a Government Requests Report reflecting its responses to government requests for data.

Google Inc. is a diversified technology company whose mission is to organize the world's information and make it universally accessible and useful. Google offers a variety of web-based products and services, including Search, Gmail, Maps, YouTube, and Blogger, that are used daily around the world. For example, more than 400 hours of YouTube videos are uploaded to Google every minute, and there are more than a billion monthly active users of Gmail. To use these and other services, users give Google information, including queries for Search, photographs for Photos, documents in Drive, emails in Gmail, videos for YouTube, and location information. Google recognizes and respects the privacy of this information and is transparent with its users about the types of data it stores when users engage with its services. Google's Privacy Policy informs

users about their data, how to keep it safe, and how to take control. And Google regularly publishes transparency reports that reflect the volume of requests for disclosure of user data that Google receives from government entities.

Microsoft Corporation is a worldwide leader in software, services, devices, and solutions, including intelligent cloud-based computing. Since its founding in 1975, Microsoft has developed a wide range of software, services, and hardware products, including the flagship Windows operating system, the Office suite of productivity applications, the Surface tablet computer, and the Xbox gaming system. Microsoft serves more than 90 markets worldwide, delivering more than 200 online services and supporting more than one billion customers from more than 100 datacenters across the globe. Microsoft is committed to its customers' privacy. Microsoft empowers its customers to control and maintain privacy of their personal data. For example, LinkedIn, a professional networking site owned by Microsoft, discloses to members which personal information it collects and gives members choices about the collection, use, and sharing of data—from controlling what data is publicly available to managing who can see when members are active on LinkedIn. Microsoft will not disclose a customer's personal data unless required by law or when necessary to protect the safety and security of its customers and services. Microsoft issues biannual transparency reports regarding requests from law enforcement for user data.

Mozilla is a global, mission-driven organization that works with a worldwide community to create open-source products such as the Firefox browser. Several hundred million users use Firefox to discover, experience, and connect to the Internet. Mozilla also operates

web services such as Firefox Accounts and Firefox Sync, which allow users to synchronize information like bookmarks and browsing history across devices, and Mozilla Location Services, which allows a device to determine their physical location. Mozilla's guiding principles recognize that individuals' security and privacy on the Internet are fundamental and not optional. Mozilla has therefore adopted data-privacy principles that emphasize transparency, user control, limited data collection, and multi-layered security control and practices. For example, Mozilla uses pseudonymous random identifiers, end-to-end encryption, and other tools because users expect their browsing information to remain private.

Nest Labs builds hardware, software, and services for the connected home. The Nest Learning Thermostat, Nest Protect smoke and carbon-monoxide alarm, and Nest Cam security camera can all be controlled remotely by customers, and Nest algorithms use data about customer's devices and activity to automate and optimize device behavior to make users' experience of the product richer and more personal. For example, the Nest Learning Thermostat collects data about users' heating and cooling patterns, as well as household occupancy and patterns. Similarly, Nest Cam can record video and audio of a home and can recognize and record when it sees a familiar person. The data may be collected either actively when the user submits it to Nest, or passively in the everyday use of the product. Nest is transparent about the types of data it stores and commits to sharing personal data only with the user's permission. Nest notifies users about legal demands when appropriate, unless prohibited by law or court order, and if a request is overly broad, Nest will

seek to narrow it. Where possible, Nest will direct government entities to the user rather than to Nest.

Oath, a subsidiary of Verizon, is a values-led company committed to building brands people love. As a global leader in digital and mobile technology, Oath reaches over one billion people around the world with a dynamic house of more than fifty media and technology brands, including Aol, HuffPost, TechCrunch, Tumblr, and Yahoo. Oath may collect IP addresses and device-location data, among other information, from its mobile users. Oath carefully reviews law-enforcement demands for user data as part of its commitment to maintaining strong and meaningful privacy protections.

Snap Inc. operates the mobile application Snapchat. With more than 150 million daily active users, Snapchat is one of the world's leading camera applications. Snapchat empowers its users to create videos and photos that help them tell their stories and talk with their friends. As with any mobile application, users' interactions with these features generate data that may be of interest to law enforcement. Snap is committed to its users' privacy, and releases transparency reports twice a year to show how the company has responded to law-enforcement requests for user data.

Twitter, Inc. operates a global platform for self-expression and communication, with the mission of giving everyone the power to create and share ideas and information instantly, without barriers. Twitter's more than 300 million active monthly users use the platform to connect with others, express ideas, and discover new information. Hundreds of millions of short messages (known as "Tweets") are posted on Twitter every day. One of Twitter's core values is defending and respecting the user's voice through a two-part commitment to

freedom of expression and privacy, including allowing users to speak pseudonymously. Steps Twitter takes to defend and respect its users include notifying users about requests for their information, giving people access to their account data, challenging legal demands to disclose user information or remove content, and having clear guidelines for appropriate uses of Twitter's interface and products. Twitter also releases regular transparency reports detailing government requests for user data.

Verizon is a global leader delivering innovative communications and technology solutions. In the United States, Verizon's award-winning wireless network affords our more than 100 million connected devices a fast, reliable network to make phone calls and consume ever-increasing amounts of data and video. When a customer uses her phone for a call or data session, the specific cell sites with which the customer's device communicates are recorded in Verizon's network records. Last year, law enforcement obtained approximately 40,000 warrants or court orders to require Verizon to provide such cell-site location information to aid them in identifying the location of a device and, presumably, its user. Verizon believes that such demands present important questions about the proper balance between security and privacy. Verizon is committed to maintaining strong and meaningful privacy protections for its customers. Verizon thus carefully reviews law-enforcement requests for user data and publishes biannual transparency reports to disclose how it has responded to those requests.

SUMMARY OF ARGUMENT

The Internet and Internet-connected devices have revolutionized nearly every facet of our lives.

Americans rely daily on services made possible by networked technologies—from email, smartphones, and web-based social media the Court has already encountered to new and evolving products and applications in the "Internet of Things," such as smart-home devices that can be used to control room temperature and lighting, order groceries, and perform a multitude of other tasks. These devices and services not only confer immense value on users and society, but in many instances are considered practical necessities of modern life.

Using these technologies often involves transmitting highly personal information through the networks and applications of digital service providers. That includes transmission of metadata—*i.e.*, data about data—generated by automated processes that are part of the background operation of digital devices and applications. Such transmissions are inherent features of how the Internet and networked devices work. Short of forgoing all use of digital technologies, they are unavoidable. And this transmission of data will only grow as digital technologies continue to develop and become more integrated into our lives. Because the data that is transmitted can reveal a wealth of detail about people's personal lives, however, users of digital technologies reasonably expect to retain significant privacy in that data, notwithstanding that technology companies may use or share the data in various ways to provide and improve their services for their customers.

Fourth Amendment doctrine must adapt to this new reality. Although amici do not take a position on the outcome of this case, they believe the Court should refine the application of certain Fourth Amendment doctrines to ensure that the law realistically engages with Internet-based technologies and with people's expectations of privacy in their digital data. Doing so

would reflect this Court's consistent recognition that Fourth Amendment protections, governed as they are by reasonable expectations of privacy, must respond to changes in technology that implicate privacy. Indeed, in declining to extend the search-incident-to-arrest exception to searches of cell phones in *Riley* v. *California*, 134 S. Ct. 2473 (2014), this Court has already signaled that digital information deserves special consideration, largely because Internet-connected devices such as smartphones "are not just another technological convenience," but are necessary to participate in the modern world, and "hold for many Americans 'the privacies of life.'" *Id.* at 2494-2495.

In the digital context, inflexible doctrines that categorically foreclose any protection for data automatically generated by ordinary digital activity—or that will be generated by the yet-to-be-conceived technologies of tomorrow—are not sustainable. In particular, the analog-era notion that transmission of data to a third party is necessarily "voluntary" conduct that precludes Fourth Amendment protection should not apply in a world where devices and applications constantly transmit data to third parties by dint of their mere operation. No constitutional doctrine should presume that consumers assume the risk of warrantless government surveillance simply by using technologies that are beneficial and increasingly integrated into modern life. Similarly, the fact that certain digitally transmitted information might have been traditionally classified as "non-content" should not unconditionally bar Fourth Amendment protection, as this data can often be highly revealing of the intimate details of a user's life.

Rather than adhere to rigid Fourth Amendment "on/off" switches developed in the analog context,

courts should take a more flexible approach that realistically reflects the privacy people expect in today's digital environment. Consistent with the general reasonable-expectation-of-privacy inquiry, courts should focus on the sensitivity of the data at issue and the circumstances of its transmission to third parties. That approach would better reflect the realities of today's digital technologies and accommodate the technologies of the future.

ARGUMENT

I. FOURTH AMENDMENT DOCTRINE MUST ADAPT TO THE CHANGING REALITIES OF THE DIGITAL ERA

"It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo* v. *United States*, 533 U.S. 27, 33-34 (2001). "The forces and directions of the Internet are so new, so protean, and so far reaching that courts must be conscious that what they say today might be obsolete tomorrow." *Packingham* v. *North Carolina*, 137 S. Ct. 1730, 1736 (2017). This Court has therefore repudiated "mechanical interpretation of the Fourth Amendment"—woodenly applying doctrines developed in one context to materially different contexts—because doing so would leave reasonable expectations of privacy "at the mercy of advancing technology." *Kyllo*, 533 U.S. at 35. Fourth Amendment law, influenced as it is by societal expectations, must account for new technology that affects those expectations.

Digital interconnectedness defines modern society. When this Court decided the cases that form the basis of the third-party doctrine—*United States* v. *Miller*, 425 U.S. 435 (1976), and *Smith* v. *Maryland*, 442 U.S.

735 (1979)—the Internet did not exist, people made calls from shared public payphones, and third-party disclosure was rarely necessary for conducting daily activities. And when Congress enacted the Stored Communications Act (SCA) in 1986, few people used the Internet, almost none had portable computers, and only around 500,000 Americans subscribed to basic cell-phone service. *See, e.g.*, CTIA, *Semi-Annual Wireless Industry Survey* 2 (2011). Today, in contrast, the vast majority of Americans—over 95% of adults—own cell phones, and 77% own smartphones. Pew Res. Ctr., *Mobile Fact Sheet* (Jan. 12, 2017). "[A] growing share of Americans now use smartphones as their primary means of online access at home." *Id.* These phones regularly transmit more data in a span of minutes than could fit on an entire hard drive in 1986. People send and receive 269 billion emails each day worldwide. Radicati Group, *Email Statistic Report, 2017-2021* (2017). Unlike the era of payphones or the early days of the SCA, many people now use the Internet and Internet-connected devices and applications to facilitate all aspects of their lives—from personal communications to shopping to tracking their health and managing their homes.

Amid these changes, as discussed below, expectations of privacy in one's personal information vis-à-vis the government have not diminished. Transmitting personal data to the companies that provide digital products and services is an unavoidable condition of using technologies that people find beneficial and useful, and forgoing the use of those technologies for many is not an option. *See, e.g.*, OECD, *Bridging the Digital Divide* (collecting articles on "[t]he risks] ... of being disconnected" due to "gaps in access to information and communication technology"). But that data can often

reveal details about the user's personal life and activities and therefore can require Fourth Amendment protection.

A. Digital Data And Devices Are Pervasive, Personal, And Often Necessary To Modern Life

Digital technologies have become a necessary aspect of life today. As many courts have recognized, the "[u]se of the Internet is vital for a wide range of routine activities in today's world—finding and applying for work, obtaining government services, engaging in commerce, communicating with friends and family, and gathering information on just about anything, to take but a few examples." *United States* v. *LaCoste*, 821 F.3d 1187, 1191 (9th Cir. 2016); *see also, e.g.*, *United States* v. *Sofsky*, 287 F.3d 122, 126 (2d Cir. 2002) ("'[C]omputers and Internet access have become virtually indispensable in the modern world.'"). Many people own cell phones simply to access the Internet and use online services. Anderson, *6 Facts About Americans and their Smartphones*, Apr. 1, 2015; *see also Riley*, 134 S. Ct. at 2489.

The Internet and Internet-connected devices have become fundamental tools for participating in many forms of modern-day activity. People now communicate by emails, text messages, and instant messaging. In the workplace, digital access has become a basic prerequisite of many jobs. *E.g.*, Dewey, *How Many Hours of Your Life Have You Wasted on Work Email?*, Wash. Post, Oct. 3, 2016 (average American white-collar worker spends 4.1 hours daily checking email); *United States* v. *Figueroa*, 2008 WL 5423982, at *2 (E.D. Wis. Dec. 30, 2008) ("Computers, internet access, and email have become indispensable parts of the functioning of this court."); Marya, *Cellphones are now essentials for*

the poor, USA Today, Sept. 14, 2013 (describing use of cell phones "to follow up on job and housing leads, and to keep in touch with public assistance agencies"). In the marketplace, digital technology offers enormous freedom for consumers in many areas of economic life. *See* Pew Res. Ctr., *Online Shopping and E-Commerce* (Dec. 16, 2016).

Digitally based activity is increasingly and quintessentially personal. Whereas in 1986 digital technologies were primarily used for business purposes, Bowman, *A Way Forward After* Warshak, 27 Berkeley Tech. L.J. 809, 809 (2012), today personal data, relationships, and intimate interactions predominate. Using digital platforms, people communicate with family and friends about their own and their children's whereabouts and activities. They share updates and exchange messages with old friends. They use cloud storage to archive notes and photos. And they network with peers, organize events, and engage in civic activity. Billions of people use social media and the Internet to "connect with one another" and "contribute to their local communities." Facebook, *Two Billion People Coming Together on Facebook*. "Seven in ten American adults use at least one Internet social networking service," *Packingham*, 137 S. Ct. at 1735, and more than 3.5 billion photos are shared daily over social media, Meeker, *2016 Internet Trends Report* 90, Kleiner Perkins Caufield & Byers (June 1, 2016).[2]

---

[2] Although using social media may sometimes involve broadcasting certain information to the public, most platforms also allow private posts or communications. Moreover, social media can implicate metadata—the result of automatic data processing that occurs "under the hood" of digital technology—that people can be unaware of or otherwise expect to remain private. *See, e.g.*,

Digital devices are also increasingly used for home-automation technology. Examples include voice assistants, such as Google Home and Apple's HomeKit and Siri, that can control room lighting and temperature, play music, or order groceries, among other functionalities, as well as cloud-based security systems and cameras, such as Nest Cam. *See* Crist, *Home Automation Buying Guide*, CINet (Apr. 28, 2017 9:07 a.m.); Wasik, *In the Programmable World, All Our Objects Will Act As One*, May 14, 2013; *see also* Note, *If These Walls Could Talk*, 130 Harv. L. Rev. 1924, 1939-1945 (2017).

Such technologies exemplify the growing "Internet of Things" (IoT): an interconnected network of "smart" devices "used to communicate and process information to an extent that was not possible before." GAO, *Internet of Things* 1 (2017) (*GAO IoT Report*). IoT devices include wearable technology such as fitness trackers and smartwatches, medical equipment and transportation infrastructure, and items in the home including coffee makers, washing machines, headphones, and lamps. This network of "rapidly proliferating ... sensors and control devices ... leverage higher capacity and higher quality wireless technology and meshed networks to add unimaginable amounts of data and ubiquitous connectivity." *NSTAC Report to the President on Emerging Technologies: Strategic Vision Executive Summary* (May 18, 2017). A "smart" thermostat, for example, can allow homeowners "not only to remotely adjust the home's temperature, but also gather data on motion, temperature, and light, and analyze those data to

---

Warner, *Protect Your Online Privacy by Removing Exif Data from Your Photos*, Que Publ'g (May 15, 2014); *see also infra* pp. 17-19.

automate the thermostat to respond to changes in the home's environment and use." *GAO IoT Report* 1.

As all these examples suggest, to withdraw from the digital arena would be to deny oneself participation in "a revolution of historic proportions," giving up access to "full dimensions and vast potential to alter how we think, express ourselves, and define who we want to be." *Packingham*, 137 S. Ct. at 1736. Forgoing the use of networked devices would "render[] modern life ... exceptionally difficult." *United States* v. *Holm*, 326 F.3d 872, 878 (7th Cir. 2003); *see also, e.g.*, *United States* v. *Dotson*, 715 F.3d 576, 586 (6th Cir. 2013). And it would "constrain[] ... freedom in ways that make it difficult to participate fully in society and the economy." *LaCoste*, 821 F.3d at 1191.

B. Users Of Digital Technologies Cannot Avoid Transmitting Sensitive Data To Service Providers, But They Expect That Data To Remain Private

"The Internet is essentially made of a big web of routers talking to each other." Parlante, *The Internet-TCP/IP, CS101—Introduction to Computing Principles*. It operates through varied and complicated forms of communication and information exchange between different parties and devices. *Id.*; *see also* Bellovin, *It's Too Complicated: How the Internet Upends* Katz, Smith, *and Electronic Surveillance Law*, 30 Harv. J.L. & Tech. 1, 5, 32-92 (2016). Using the Internet to make a call, send a message, or retrieve information means "talk[ing]" to other computers by sending packets of data and interacting with various layers of system protocols and architecture. Shuler, *How Does The Internet Work?* "[E]ven within a single device, different layers

may be operated by different parties." Bellovin, 30 Harv. J.L. & Tech. at 33.

By virtue of that architecture and the way the Internet and wireless networks operate, all digital technology transmits user information to various service providers. Those transmissions are an unavoidable condition of using digital technology. But in this digital era, users may not expect or intend that, by relying on service providers to administer everything from their email content and address book to their health and fitness data, they assume the risk that the government could amass and monitor their data without a warrant. *See, e.g.*, Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era* 34 (Nov. 14, 2014) (most study respondents thought of their location information as private).

The data transmitted may be highly sensitive. As this Court has observed with respect to established technologies, "[a]n Internet search and browsing history ... [can] reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD." *Riley*, 134 S. Ct. at 2490. Similarly, "[h]istoric location information"—something not unique to cell phones—"can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Id.* (citing *United States* v. *Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.")). The same is true of other new and evolving technologies. To improve energy efficiency, a smart thermostat detects and transmits not just a home's temperature, but information

about the homeowner's habits—whether and when the occupants are home, and where they are in the home. And to improve home security, smart security cameras can develop the ability to recognize individuals and record and transmit information about their comings and goings.

Whether email, cloud computing, location-based tracking, or any other digital functionality is at issue, users consider many types of collected electronic data to be private—particularly given the personal details that information can reveal—regardless of whether transmission to a third party has occurred behind the scenes in the creation or processing of that data. *See* Mastroianni, *Survey: More Americans Worried About Data Privacy than Income*, CBS News, Jan. 28, 2016. User and market research, including extensive review of user feedback and complaints, confirms this expectation.[3]

Even on social-media platforms such as Facebook and Twitter, privacy settings allow users to control whether their posts will be disclosed publicly, only to specified friends and family, or not at all. And even

---

[3] According to a poll by the Pew Research Center, "93% of adults say that being in control of who can get information about them is important: 74% feel this is 'very important'; 19% say it is 'somewhat important.' 90% say that controlling what information is collected about them is important—65% think it is 'very important' and 25% say it is 'somewhat important.'" Madden, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Res. Ctr., May 20, 2015. Additionally, "Americans say they do not wish to be observed without their approval; 88% say it is important that they not have someone watch or listen to them without their permission (67% feel this is 'very important' and 20% say it is 'somewhat important')." *Id.*

when posting publicly, users may not expect metadata encoded within those posts to be available to the government without a warrant. *Supra* p. 15-16 n.2. Indeed, for some platforms, privacy controls are at the heart of the service provided. For example, the Snapchat app, from its very beginning, was designed to give individuals a way of expressing themselves and communicating with others without creating a permanent record of the expression. In this way, the app protects individuals' privacy by deleting many communications and content by default once they have been viewed by the recipient. Snap further protects its users' privacy by encrypting the most sensitive data while it is stored, including location data, "Snaps," and "Stories."

Because amici recognize the sensitivity of the data their users entrust to them, they work diligently to protect customer information and take substantial measures to honor and reinforce their customers' expectation of privacy. These measures include offering user-controlled privacy settings, providing robust data encryption, and employing teams of data-security specialists to protect their systems from unauthorized access.[4] Many amici subject themselves to external audits of their infrastructure, applications, and operations to ensure the highest levels of protection of user data.[5] The reason for these measures is simple: While amici's customers understand that data is collected by service providers as part of providing digital technologies,

---

[4] *See, e.g.*, Google, *Privacy*; Apple, *Privacy Policy*; *Dropbox Privacy Policy*.

[5] *See, e.g.*, Google, *Cloud Platform Security*; Microsoft Trust Center, *Security, Audits, and Certifications*.

customers still expect privacy with respect to other parties, including the government.

C. Amici's Compliance With Law-Enforcement Requests Respects User Privacy

When law-enforcement agencies seek user data pursuant to a warrant—which, for example, has been routine with regard to email for some time—amici work to ensure that investigative needs are met without subjecting users to undue intrusion.[6] Where appropriate, amici voluntarily challenge overbroad or unsupported requests; but they also regularly turn digital information over to law enforcement in response to valid warrants. For example, Apple "carefully reviews all requests from government, law enforcement, and private parties to ensure that there's a valid legal basis for

---

[6] The SCA, 18 U.S.C. § 2703(a), generally requires law enforcement to obtain a warrant based on probable cause to access the "contents" (but not "records," *see id.* § 2703(c); *infra* p. 30 n.8) of electronic communications. Although Section 2703(b) of the Act allows law enforcement to use lesser legal process for certain types of communications under certain conditions, that subsection has been held unconstitutional, *see United States* v. *Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), and the Department of Justice has followed that holding as a matter of policy since 2013 by using only warrants to obtain stored content, H.R. Rep. No. 114-528, at 9 (2016). As this Court has noted, digital technologies make it easier for law-enforcement officers to secure warrants. *See Missouri* v. *McNeely*, 133 S. Ct. 1552, 1562 (2013); *see also Riley*, 134 S. Ct. at 2493. Federal Rule of Criminal Procedure 4.1 and "a majority of States" allow law-enforcement officials "to apply for search warrants remotely through various means, including telephonic or radio communication, electronic communication such as e-mail, and video conferencing." *McNeely*, 133 S. Ct. at 1562. Telephonic or email warrants can be obtained within the time of the average traffic stop. *See, e.g.*, *State* v. *Zeller*, 172 Wash. App. 1008 (2012).

each request." Apple, *Legal Process Guidelines: Government & Law Enforcement Within the United States*. Should it "determine[] that there is no valid legal basis or ... [that the] request is ... unclear, inappropriate or over-broad[,] Apple will challenge or reject the request." *Id.*

All amici practice and support this approach. *See, e.g.*, Dropbox, *Transparency Overview* ("Government data requests should be limited in the information they seek and narrowly tailored to specific people and legitimate investigations. We'll resist blanket and overly broad requests."); Apple, Lithium Techs., Mozilla, and Twilio Amicus Br. 11-12, Dkt. 66-1, *Microsoft* v. *United States*, No. 16-cv-00538 (W.D. Wash. Sept. 2, 2016) (discussing service providers' standing and practices to "challenge various forms of legal process served upon [companies] seeking customer data").

Amici also strive to be fully transparent about their interactions with law enforcement. *Supra* pp. 2-9. For instance, most amici notify users about requests for their data unless legally prohibited from doing so, and most amici publish transparency reports that detail the number and types of requests amici have received from government agencies and how they have responded to those requests.[7] These steps require an investment of time, energy, and resources. Yet amici take them because their users care about the privacy of their data and have made clear their "societal understanding that certain areas"—including in the digital realm—"deserve the most scrupulous protection from govern-

---

[7] *See, e.g.*, Apple, *Report on Government and Private Party Requests for Customer Information*; Snap, *Transparency Report*; Twitter, *Transparency Report: United States*.

ment invasion." *Oliver* v. *United States*, 466 U.S. 170, 178 (1984).

II. Rigid Analog-Era Rules Should Yield To Consideration Of Reasonable Expectations Of Privacy In The Digital Age

A. A Flexible Test Grounded In Today's Reasonable Expectations Of Privacy Should Govern In The Digital Context

As the foregoing discussion illustrates, when customers transmit personal data to technology companies in the course of using digital products and services, they reasonably expect that data and the metadata generated alongside it to be securely stored and remain private as to the rest of the world. They should not be forced to relinquish Fourth Amendment protections against government intrusion simply by choosing to use those technologies. To resolve this case, the Court should forgo reliance on outmoded rules that make little sense when applied in the digital context. In particular, the third-party doctrine and the content/non-content distinction should not operate to categorically foreclose Fourth Amendment protection; instead, Fourth Amendment law should favor a more flexible approach that assesses reasonable expectations of privacy in light of new and evolving technologies and the highly sensitive data they implicate.

"[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish," *Warshak*, 631 F.3d at 285—a point this Court has recognized and applied on more than one occasion. For example, where previously the Fourth Amendment's protections applied only to common-law trespass and physical seizure, this

Court held half a century ago that the widespread adoption of telephones "so eroded" that approach that it "c[ould] no longer be regarded as controlling." *Katz* v. *United States*, 389 U.S. 347, 351-353 (1967); *see also id.* at 361-362 (Harlan, J., concurring); *Jones*, 565 U.S. at 404-411. As the Court recognized, "[t]o read the Constitution more narrowly"—and allow law enforcement to eavesdrop unfettered on a caller "surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world"—would impermissibly "ignore the vital role that the public telephone has come to play in private communication." *Katz*, 389 U.S. at 352.

The Court should take similar account of the effects of the Internet and other digital technologies. Just as the widespread adoption of the telephone in the twentieth century required the Court to cabin obsolete Fourth Amendment doctrine in *Katz*, in the twenty-first century, Fourth Amendment doctrine must accommodate a historic shift in the use of digital technology. This Court has already taken a large step in that direction. In *Riley*, 134 S. Ct. 2473, the Court recognized the all-encompassing and private nature of digital data in holding that "officers must generally secure a warrant" before conducting a search for data on a cell phone. *Id.* at 2485. The Court reasoned that while the general rule allowing warrantless searches incident to arrest "strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones." *Id.* at 2484. Consequently, the Court declined to extend that rule to "searches of data on cell phones," instead requiring a warrant. *Id.* at 2485.

Fundamental to the Court's decision in *Riley* were two factors that apply as well to other digital technolo-

gies. First, the Court observed that "[m]odern cell phones are not just another technological convenience," but rather have become "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley*, 134 S. Ct. at 2484, 2494. Second, the Court recognized that cell phones "hold for many Americans 'the privacies of life.'" *Id.* at 2494-2495; *see also id.* at 2488-2491.

As discussed above, those considerations apply with equal or greater force to other digital technologies. As to the first, Internet-based services and devices are ubiquitous and "virtually indispensable in the modern world of communications and information gathering." *United States* v. *Peterson*, 248 F.3d 79, 83 (2d Cir. 2001) (per curiam); *see United States* v. *Voelker*, 489 F.3d 139, 145 (3d Cir. 2007); *supra* Part I.A. And as to the second, digital devices and services produce and record data that, alone or in the aggregate, has the potential to reveal highly sensitive information about all aspects of our private lives. *Supra* Part I.B. Accordingly, rather than automatically disqualifying digital data from Fourth Amendment protection based on rigid analog-era rules, courts should focus on the fundamental Fourth Amendment question: whether an individual has a reasonable expectation of privacy in a given set of digital data. In answering that question, courts should consider among other things the degree to which the data has the potential to reveal intimate details about the user, *see, e.g.*, *Riley*, 134 S. Ct. at 2490; *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring); *Kyllo*, 533 U.S. at 34-36 & n.4, 40; *United States* v. *Karo*, 468 U.S. 705, 715 (1984), and the extent to which the service or device is used by the average person, *cf. Riley*, 134 S. Ct. at 2484.

This approach has the virtues of assessing digital data on its own terms and realistically engaging with the reasonable expectations of privacy of modern Americans. And it affords courts an adaptable method of analysis that will remain workable even as digital technology evolves. *Packingham*, 137 S. Ct. at 1736.

B. Transmission To A Service Provider Should Not Automatically Foreclose Protection Of Digital Data

The third-party doctrine is the notion that Fourth Amendment protection does not extend to information voluntarily disclosed to a third party. In *Smith*, 442 U.S. 735, for example, the Court rejected Fourth Amendment protection for telephone numbers recorded by pen register, which had "limited capabilities"—indeed, "'[n]either the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed [could be] disclosed.'" *Id.* at 741. The decision rested on the caller's conveyance of the numbers to his telephone company through early switchboard equipment, which the Court analogized to giving information to a live operator. *Id.* at 745. Similarly, in *Miller*, 425 U.S. at 442, the Court declined to extend Fourth Amendment protection to "negotiable instruments to be used in commercial transactions" when those instruments had been given to a bank. The Court explained that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party," "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* at 443. Courts have extrapolated from these decisions a "binary" inquiry "in which any information dis-

closed to a third party for any reason is public and does not merit Fourth Amendment protection." Note, *If These Walls Could Talk*, 130 Harv. L. Rev. at 1931.

This rigid interpretation is unworkable when applied to the Internet and digital technologies, which operate through varied and complicated forms of information exchange between different parties and devices. *See Jones*, 565 U.S. at 417-418 (Sotomayor, J., concurring); Note, *If These Walls Could Talk*, 130 Harv. L. Rev. at 1933-1937. Unlike the "limited capabilities" of pen-register data, *Smith*, 442 U.S. at 742, the data transmitted by users of digital devices and applications can often reveal intimate details of people's lives, especially when viewed in the aggregate. Cell-tower records that reveal a person's general location are but the tip of the iceberg. People search online for all manner of information, including medical advice, and rely on the Internet for their jobs, schooling, and interpersonal communications. They reveal their habits, views, and preferences by interacting with apps used to navigate almost every facet of their lives. They store photos and emails in the cloud, rely on data-collecting devices such as fitness trackers to manage their health, and use smart appliances to provide home security and efficiency. For many of these activities, there is no analog-era analogy; in the past, for instance, a user did not have to tell a company when and how he wanted to adjust his thermostat, thereby risking losing all privacy protection in that information.

The incongruity between the third-party doctrine and reasonable expectations of privacy is only amplified in the context of home-automation devices and other smart-home technology, which bring connectedness into private spaces. *See supra* pp. 7, 10, 13, 16-17, 18-19. "'At the very core' of the Fourth Amendment

'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" *Kyllo*, 533 U.S. at 31; *see also, e.g.*, *Karo*, 468 U.S. at 714 ("[P]rivate residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable."); Pesciotta, *I'm Not Dead Yet:* Katz, Jones, *and the Fourth Amendment in the 21st Century*, 63 Case W. Res. L. Rev. 187, 217-219 (2012) ("the Court has always been steadfast in its protection of privacy in the home—an area in which all citizens undoubtedly expect the utmost level of privacy").

Moreover, the premise of the third-party doctrine—that what one voluntarily and knowingly exposes to another is no longer private—bears little relevance to many modern technologies. As discussed, many devices and applications transmit data automatically with no prompting by the user. *See supra* pp. 10, 15-16 n.2, 17-19. In addition, digital data, whether passively or actively conveyed, often is not really "exposed" to others or directly observed by another human being, but is instead automatically transmitted and processed by different computer software and servers. And as discussed, these transmissions are a necessary condition of participating in the digital world.

Finally, treating such disclosures as a voluntary relinquishment of privacy for all purposes is misconceived because it allows no possibility for degrees of privacy. In the digital era, "[p]rivacy is not a discrete commodity, possessed absolutely or not at all." *Smith*, 442 U.S. at 749 (Marshall, J., dissenting). Engaging in activities that expose personal information to one audience does not diminish the reasonable expectation that one's personal information should otherwise remain private.

That users rely on technology companies to process their data for limited purposes does not mean that they expect their intimate data to be monitored by the government without a warrant. As one court aptly observed, "[h]otel guests, for example, have a reasonable expectation of privacy in their rooms ... even though maids routinely enter hotel rooms to replace the towels and tidy the furniture," and "tenants have a legitimate expectation of privacy in their apartments ... regardless of the incursions of handymen to fix leaky faucets." *Warshak*, 631 F.3d at 287; *see also* Colb, *What Is A Search?*, 55 Stan. L. Rev. 119, 122-123 (2002). In using digital technologies, too, people can and do reasonably expect certain information to be kept private with regard to one audience or purpose but not with regard to another—particularly when that data is highly revealing of intimate details and cannot be kept entirely from others without forgoing the use of digital technologies.

C. "Non-Content" Digital Data Should Not Automatically Be Excluded From Protection

The content/non-content distinction is the idea that, although the content of communications themselves, such as the text of a letter, is considered private and subject to Fourth Amendment protections, the "non-content" information necessary to process the communication or route it from one point to another—*e.g.*, the address on the outside of the envelope—is not. Thus, in *Ex parte Jackson*, 96 U.S. 727 (1878), the Court held that postal inspectors needed a search warrant to open letters and packages, but that the "outward form and weight" of those mailings were not constitutionally protected. *Id.* at 773. This distinction rests on the notion that non-content routing information is limited in what

it reveals about a person and is visible in plain view. *See id.*

Amici agree that content, digital or otherwise, should receive strong protection under the Fourth Amendment. *See Warshak*, 631 F.3d at 285-286. An email is no less personal and revealing, and no more out in the open, than the contents of a physical letter or telephone call. "Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection." *Id.* But the notion that "non-content" information should automatically be relegated to a less-protected status ignores the realities of digital data.[8]

The cell-site location data at issue here can reconstruct the user's movements, revealing significant information about the user's associations and activities. *Riley*, 134 S. Ct. at 2490; *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). Indeed, the detail revealed by such data is even greater today than it was just six years ago when law enforcement sought access to information from Mr. Carpenter's device. Since then, as the number of smartphones and the volume of data usage have dramatically increased, Verizon has expanded its network and added smaller cell sites, which have narrower ranges than larger, traditional cell towers

---

[8] The SCA—enacted more than thirty years ago—distinguishes between contents of communications and records concerning communications by requiring the full protections of a warrant only for the former. *See* 18 U.S.C. § 2703. But that statute was not written with today's digital landscape in mind, and it is not dispositive of the constitutional question whether there is a reasonable expectation of privacy in digital data.

and "fill in coverage gaps between larger towers." Silliman, *Musing About the Third Party Doctrine During Network Planning Meetings* (Oct. 10, 2016). As a result, Verizon's network now collects even more voluminous and much more precise location information capable of providing a wealth of detail. *Cf. United States* v. *Pineda-Moreno*, 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, J., dissenting) ("Are Winston and Julia's cell phones together near a hotel a bit too often? Was Syme's OnStar near an STD clinic? Were Jones, Aaronson and Rutherford at that protest outside the White House?").

That said, the sensitivity of digital data is hardly limited to location information. Some types of data that digital devices generate may reveal with considerable precision granular details about the materials people read, the precise actions they take on their devices, and much more. *Riley*, 134 S. Ct. at 2490. Moreover, digitally encoded information is hardly in plain view. It requires special equipment and software to piece together.

For example, when an Internet user opens a news story, views a photograph, or sends a message to a friend, the user's smartphone often makes a record of that action, and those records are often transmitted to third parties such as the operator of the Internet platform or mobile application. Arguably, these records are not "content" in the analog sense; they do not contain communications in sentence or paragraph form. But they have the potential to reveal highly private and personal information about the user.[9] A law-

---

[9] Given the content/non-content distinction's analog pedigree, courts have struggled to classify certain types of data. URLs are

enforcement agent who accesses such records about John Smith would know what news stories Smith read, what photographs he viewed, and when and from where he sent those messages. Government agencies could try to use log data from a search engine that would show a user's pattern of accessing websites about anorexia, mental health, or substance-abuse treatments. Data from a connected security systems or other smart-home devices could reveal when the user is out of town. Even the metadata recording the delivery information of a single email message could expose the membership of an entire political organization. *Cf. NAACP* v. *Alabama*, 357 U.S. 449 (1958).

Even if it could be considered "non-content," this data can be as revealing about the intimate details of one's life as the actual content of a message. It makes little sense to subject such sensitive data, which is both quantitatively and qualitatively "different" from any analog notion of routing information for telephones or snail mail, *Riley*, 134 S. Ct. at 2490, to a rule developed in the pre-digital context, where the risks of revealing deeply personal information were indisputably lower.

CONCLUSION

The Court should afford strong Fourth Amendment protection to digital data and reject mechanical application of the third-party doctrine and content/non-content distinction in favor of a more flexible analysis

---

a good example: "Though some district courts have held that a URL is never content," other courts have found that certain types of URLs could be content depending on the information they reveal. *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 138 (3d Cir. 2015).

that takes account of people's reasonable expectations of privacy in the digital era.

Respectfully submitted.

SETH P. WAXMAN
Counsel of Record
JONATHAN G. CEDARBAUM
CATHERINE M.A. CARROLL
ROBBIE MANHAS
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Ave., NW
Washington, DC 20006
(202) 663-6000
seth.waxman@wilmerhale.com

AUGUST 2017

RECORD AND BRIEFS

No. 16-402

Supreme Court, U.S.
FILED
AUG 14 2017
OFFICE OF THE CLERK

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

BRIEF OF TECHNOLOGY EXPERTS AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

BRIAN WILLEN
JACK MELLYN
SAMUEL DIPPO
WILSON SONSINI GOODRICH & ROSATI
1700 K Street NW
Washington, DC 20002
(202) 973-8800

ALEX ABDO
Counsel of Record
JAMEEL JAFFER
KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY
535 West 116th Street
314 Low Library
New York, NY 10027
(212) 854-9600
alex.abdo@knightcolumbia.org

Counsel for Amici Curiae

TABLE OF CONTENTS

Page

TABLE OF CONTENTS i

TABLE OF CITED AUTHORITIES iii

INTRODUCTION 1

INTERESTS OF AMICI 1

SUMMARY OF ARGUMENT 5

ARGUMENT 6

I. CELL SITE LOCATION INFORMATION IS BECOMING INCREASINGLY DETAILED, CONTEMPORANEOUS, AND PRECISE 6

A. Cell Phones Have Become An Essential Part of American Life 7

B. Cell Phones Constantly Generate Highly Detailed Information On Users' Locations and Movements 9

1. Law Enforcement Frequently Obtains Both Historic and Real-Time CSLI 10

C. CSLI is Routinely Collected Without User Knowledge or Consent 13

Table of Contents

Page

D. CSLI is Precise and Becoming More So Every Year 14

1. Increases in CSLI Precision Are Being Driven by Continuing Improvements in Network Architecture 14

2. The New Generation of Cell Networks Will Allow Increasingly Detailed CSLI 19

3. Carriers Are Storing Increasingly Large Amounts of CSLI and Analyzing this Data Is Increasingly Easy 22

II. CELL SITE LOCATION INFORMATION REVEALS AN EXTRAORDINARILY DETAILED PICTURE OF AN INDIVIDUAL'S LIFE, EVERY BIT AS REVEALING AS THE CONTENT OF THEIR COMMUNICATIONS 27

A. Even Discrete Pieces of CSLI Reveal Extremely Sensitive Information 27

B. Aggregated CSLI Has the Potential to Reveal Even More Sensitive Detail 32

CONCLUSION 37

TABLE OF CITED AUTHORITIES

Page

CASES

Illinois v. Lidster,
540 U.S. 419 (2004) 25

In re United States ex. rel. an Order Authorizing the Installation & Use of a Pen Register,
402 F. Supp. 2d 597 (D. Md. 2005) 10

Katz v. United States,
389 U.S. 347 (1967) 7

Riley v. California,
134 S. Ct. 2473 (2014) 8

United States v. Garcia,
474 F.3d 994 (7th Cir. 2007) 25

United States v. Graham,
824 F.3d 421 (4th Cir. 2016) 24

United States v. Jones,
565 U.S. 400 (2012) 11, 25, 32

United States v. Maynard,
615 F.3d 544 (D.C. Cir. 2010) 32

United States v. Pineda-Moreno,
617 F.3d 1120 (9th Cir. 2010) 12

Cited Authorities

Page

United States v. Stimler,
No. 15-4095, 2017 WL 3080866
(3d Cir. July 7, 2017).....16

STATUTES AND OTHER AUTHORITIES

18 U.S.C. § 2703.....11

2016 Global Mobile Consumer Survey: US Edition,
Deloitte 7

Andrew Lipsman, *Mobile Matures as the Cross-Platform Era Emerges*, ComScore
(Mar. 31, 2017).....7

Bhavin Shah, *Polaris Wireless Solutions*, Law and
Order Mag. (July 2013) 24

Brassil et al., *Authenticating Location with Femtocells*, Mass. Inst. Tech.....28

Brian Fung, *New FCC Proposal Would Require Pinpoint Location Accuracy for 911 Calls*, Washington Post (Feb. 20, 2014).....19

Cell Phone Location Tracking Request Response - Cell Phone Company Data Retention Chart, Am. Civil Liberties Union 22

Cellular Analysis Mapping Program v2.7, Officer.com 26

Cited Authorities

Page

Charles Blain, *Police Could Get Your Location Data Without A Warrant. That Has To End*, Wired (Feb. 2, 2017, 7:00 AM).....8

Chelsea J. Carter, *Where (and When) Do You Use Your Smartphone: Bedroom? Church?*, CNN (July 13, 2013, 9:46 PM) 7, 28

Christopher Soghoian, *8 Million Reasons for Real Surveillance Oversight*, Slight Paranoia Blog (Dec. 1, 2009).....12

Conference Presentation, Mahesh Patel, *Location for Public Safety and Emergency Management*, Geo Smart Asia 2016 (Oct. 18, 2016) 23

Conference Report, Arvind Thiagarajan et. al., *Accurate, Low-Energy Trajectory Mapping for Mobile Devices*, NSDI'11 Proc. of the 8th USENIX Conference on Networked Sys. Design and Implementation (Mar. 30, 2011).....20

Craig Silliman, Exec. Vice President, Pub. Pol'y & Gen. Counsel, Verizon, *Technology and Shifting Privacy Expectations*, Bloomberg Law (Oct. 7, 2016).....18

CTIA, *Enabling the Wireless Networks of Tomorrow*.....17

Data Retention in Switzerland, Digitale Gesellschaft.....33

Cited Authorities

Page

Electronic Communications Privacy Act Hearing on ECPA, (Part II): Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. and Investigations of the H. Comm. on the Judiciary, 113 Cong. 2 (2013) . . *passim*

Enabling the Wireless Networks of Tomorrow, CTIA (Apr. 2016) 16

Events Calendar, Lutheran Church of the Reformation 31

Gavin Horn, *3GPP Femtocells: Architecture and Protocols*, Qualcomm 59 (Sept. 2010). 28

Interview by Cyrus Farivar with Malte Spitz (Jan. 4, 2011) 33

John Villasenor, *Recording Everything: Digital Storage as an Enabler of Authoritarian Governments*, Brookings (Dec. 14, 2011) 22

Joseph Hoy, *Forensic Radio Survey Techniques for Cell Site Analysis* 69 (2015) 15, 20

Kai Biermann, *Betrayed by our own data*, Zeit Online (Mar. 10, 2011, 5:09 PM) 31, 34

Cited Authorities

Page

Kate Kaye, *The $24 Billion Dollar Business That Telcos Don't Want to Talk About*, Advertising Age (Oct. 26, 2015) 23

Kenneth Lipp, *AT&T is Spying on Americans for Profit*, Daily Beast (Oct. 25, 2016, 1:13 AM) 27

Kevin Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, 123 Yale L.J. Online 335 (2014) 24, 25

Letter from Lisa A. Judge, Principal Assistant City Att'y, Tucson Police Dep't to Dan Pochoda, Am. Civil Liberties Union (Sept. 6, 2011) ... 11-12, 25

Mark Harris, *How Peter Thiel's Secret Company Secretive Data Company Pushed Into Policing*, Wired (Aug. 9, 2017) 26

Martha DeGrasse, *Can Verizon and AT&T Deploy 100,000 New Small Cells?*, RCR Wireless News (Oct. 29, 2015).....16

Massive Growth Projected for DAS Deployments, agl Media Group (Nov. 14, 2013).....17

Mobile Fact Sheet, Pew Research Center 7

Cited Authorities

Page

Monica Alleven, *Transit Wireless Wraps Latest Phase of Huge DAS System for NYC Subway Stations*, FierceWireless (Nov. 16, 2015, 9:55 AM) 17

Nathan Eagle et al., *Inferring friendship network structure by using mobile phone data*, 106-36 Proc. of the Nat'l Acad. of Sci. 15274, 15275 (Sept. 8, 2009).....35

Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. Times (Mar. 26, 2011) 33

Press Release, AT&T, Information for Public Safety (Sept. 30, 2017).....12

Press Release, Office of the Mass. Attorney General, AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities (Apr. 4, 2017).....30

Robinson Meyer, *How the Government Surveils Cellphones: A Primer*, The Atlantic (Sept. 11, 2015) 9

Robinson Meyer, *No One Will Save You From Cellphone Tracking*, The Atlantic (June 2, 2016) 11

Cited Authorities

Page

Russell Brandom, *DC Prosecutors Are Ramping Up Secret Requests for Location and Internet History*, The Verge (July 19, 2017, 1:50 PM) 11

Scott Shane and Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, N.Y. Times (Sept. 1, 2013) 27

Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards For Law Enforcement Access To Location Data That Congress Could Enact*, 27 Berkeley Tech. L.J. 117 (2012) 16

Tell-all Telephone, Zeit Online (March 2011) 33, 34

Tom Wheeler, Chairman, Fed. Commc'ns Comm'n, Remarks at CTIA Super Mobility Show 2016 (Sept. 7, 2016).....17

Transparency Report, AT&T 11

Unique Features of Pen-Link v8, Pen-Link (Apr. 17, 2008).....26

Wireless Snapshot 2017, CTIA (May 2017) 8, 15

Cited Authorities

Page

Yves-Alexandre de Montjoye et al., *Predicting Personality Using Novel Mobile Phone-Based Metrics*, *in* Social Computing, Behavioral-Cultural Modeling and Prediction 48, 49 (A.M. Greenburg et al. eds, 2013) 34-35

Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Scientific Reports (Mar. 25, 2013) . . . 21, 32

INTRODUCTION

The ability of cellular phones to track their users' locations and movements has undergone a revolution since the first mobile networks were introduced in the 1980s. Originally capable only of identifying the general area from which a user was calling, today's cell site location information ("CSLI") is both rich and precise, opening the door for those with access to it, including law enforcement, to reconstruct the detailed movements, personal activities, habits, and associations of not just the direct targets of the surveillance but third parties as well. This data will only become more revealing over time as technology continues to develop to make CSLI more precise. Given the unique power of this data and its potential for misuse, amici urge the Court to hold that law enforcement officials must obtain a warrant under traditional Fourth Amendment standards before being permitted to access and use CSLI.

INTERESTS OF AMICI[1]

Amici are leading technology experts whose work addresses the privacy implications of modern communications tools. Amici have particular interest in and expertise regarding the rapid growth of CSLI technology and the serious privacy consequences that could result from its unrestrained acquisition and use by law enforcement. Amici submit this brief to explain the technology of CSLI location tracking, its rapidly

1. The parties have submitted blanket letters of consent to the filing of amicus briefs in this case. None of the parties authored this brief in whole or in part, and no one other than amici and their counsel made a monetary contribution to the preparation or submission of this brief.

increasing precision, and the ways in which it can be used to reveal highly detailed pictures of individual lives.

Ashkan Soltani is an independent researcher and technologist specializing in privacy, security, and behavioral economics. He previously served as a Senior Advisor to the U.S. Chief Technology Officer in the White House Office of Science and Technology Policy and as the Chief Technologist for the Federal Trade Commission.

Dr. Edward W. Felten is the Robert E. Kahn Professor of Computer Science and Public Affairs at Princeton University, and the founding Director of Princeton's Center for Information Technology Policy. In 2015–2017 he served in the White House as Deputy U.S. Chief Technology Officer. In 2011–2012 he served as the first Chief Technologist at the U.S. Federal Trade Commission. He has published more than 150 papers in the research literature, and three books.

Dr. Matt Blaze is an associate professor of computer and information science at the University of Pennsylvania in Philadelphia, where he serves as director of the Distributed Computing Laboratory and conducts research on computer security, cryptography, network communication, and surveillance technology. In 2013, he testified before the U.S. House of Representatives on the potential privacy implications of widespread access to CSLI.

Dr. Steven M. Bellovin is the Percy K. and Vida L.W. Hudson Professor of Computer Science at Columbia University. He has served as Chief Technologist of the Federal Trade Commission and as the Technology Scholar at the Privacy and Civil Liberties Board.

Bruce Schneier is an internationally renowned security technologist, called a "security guru" by the Economist. He is the author of 14 books—including the New York Times best-seller *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*—as well as hundreds of articles, essays, and academic papers.

Dr. Joseph Lorenzo Hall is the Chief Technologist and Director of the Internet Architecture project at the Center for Democracy & Technology, a Washington, DC-based non-profit advocacy organization dedicated to ensuring digital rights and that the internet remains open, innovative, and free.

Morgan Marquis-Boire is a New Zealand born security researcher and journalist. He is the Director of Security for First Look Media and a contributing writer for The Intercept.

Dr. Nicholas Weaver is a researcher focusing on security and privacy at the International Computer Science Institute in Berkeley and a lecturer in Computer Science at the University of California at Berkeley.

Dr. Stephen Checkoway is an assistant professor of computer science at the University of Illinois at Chicago where he conducts research on the security of embedded computer systems.

Dr. Dan S. Wallach is a Professor in the Departments of Computer Science and Electrical and Computer Engineering and a Rice Scholar at the Baker Institute for Public Policy at Rice University.

Adam Shostack is a consultant and the author of *Threat Modeling: Designing for Security.*

Dr. Rebecca Wright is a professor in the Computer Science Department and Director of DIMACS at Rutgers.

Dr. Carrie E. Gates is the Chief Technology Officer for an emerging Boston-based start-up focusing on providing security tools for cloud-based applications.

Scott Bradner was involved in the design, operation and use of data networks at Harvard University since the early days of the ARPANET. He retired from Harvard University in 2016 after 50 years working there in the areas of computer programming, system management, networking, IT security, and identity management.

Dr. Susan Landau is Bridge Professor in the Fletcher School of Law and Diplomacy and the School of Engineering, Department of Computer Science, Tufts University and Visiting Professor of Computer Science, University College London.

Dr. Ben Adida is the Vice-President of Engineering at Clever Inc., which specializes in securing student data in K-12 schools around the United States.

Dr. Nadia Heninger is an assistant professor in the Computer and Information Science department at the University of Pennsylvania.

Philip Zimmermann is the creator of Pretty Good Privacy, an email encryption software package, and teaches cryptography at the Delft University of Technology's Faculty of Electrical Engineering.

Dr. Sharon Goldberg is an associate professor in the Computer Science Department at Boston University. Her research focuses on practical problems in network security, and she has served on working groups of the Federal Communications Commission and the Internet Engineering Task Force.

SUMMARY OF ARGUMENT

Cell site location information is no longer confined to crude approximations, but has become increasingly sophisticated and precise. The majority of Americans now carry their phones at nearly all times, largely unaware that the devices are automatically creating a detailed and lasting record of their locations and movements. In the hands of law enforcement, these records have the potential to reveal a wide range of information about individuals' habits, activities, and associations.

The implications of unrestricted government access to CSLI for privacy and the freedoms of expression and association are profound. Even discrete pieces of CSLI can be used to uncover highly sensitive personal information—including an individual's medical conditions, religious beliefs, or political affiliations. Aggregated over time, CSLI is even more revealing, exposing an individual's social circles, romantic liaisons, and even morning and nighttime routines as they move about their house. Combined even further with publicly available data, such as maps, calendars, and social media postings, CSLI has the potential to reveal the most intimate details of a person's life.

Cellular carriers now routinely retain months and even years of CSLI data, on all of their users. And law enforcement increasingly requests large tranches of this information—making up many months—for their surveillance targets. The use of this information without adequate court supervision has the potential to profoundly unsettle legitimate expectations of privacy. Amici therefore urge the Court to treat this issue as the serious and growing challenge to individual privacy that it is, and to institute appropriate safeguards for CSLI use, including requiring law enforcement to obtain a warrant, subject to traditional Fourth Amendment standards, before obtaining or using it.

ARGUMENT

I. CELL SITE LOCATION INFORMATION IS BECOMING INCREASINGLY DETAILED, CONTEMPORANEOUS, AND PRECISE

Cellular phones have become a central part of our lives. Americans increasingly carry them everywhere, using them as a central hub for memories, work lives, and family relationships. However, these same phones broadcast a constant stream of information about their users' locations and activities—information that is frequently demanded by law enforcement and other government officials. This information—including CSLI—is far more precise and revealing now than it was in even the recent past, and will only become more so as cellular technology continues to develop.[2]

---

2. This brief (like the case) focuses on cell phones, but other devices that connect to cellular networks—including tablets, laptops, and wireless hotspots—could also generate CSLI records, as could any type of future technology relying on these networks.

A. Cell Phones Have Become An Essential Part of American Life

Like the wire-based telephone before it, the cellular telephone has come to play a singular and vital role in our private lives. Cf. *Katz v. United States*, 389 U.S. 347, 352 (1967) (crafting Fourth Amendment rules in recognition of "the vital role that the public telephone has come to play in private communication"). With 95% of Americans owning one, and more than 396 million units in circulation in the U.S. alone, the cell phone has become the most widely adopted piece of technology in our nation's history.[3] Americans not only use their phones, but carry them wherever they go, including home, work, school, the grocery store, their children's preschool, their doctors, churches, and more. In one study, 72% of respondents stated that they were within a five-foot reach of their phones for a majority of the time, with twelve percent even admitting to using their phones while in the shower.[4] We are also increasingly active on our phones. The average user spends nearly 3 hours per day on their phone,[5] while younger Americans report that they check their phones up to 82 times a day.[6]

---

3. *Mobile Fact Sheet*, Pew Research Center, http://www.pewinternet.org/fact-sheet/mobile/ (last visited Aug. 11, 1017).

4. Chelsea J. Carter, *Where (and When) Do You Use Your Smartphone: Bedroom? Church?*, CNN (July 13, 2013, 9:46 PM), http://www.cnn.com/2013/07/13/tech/smartphone-use-survey/.

5. Andrew Lipsman, *Mobile Matures as the Cross-Platform Era Emerges*, ComScore (Mar. 31, 2017), http://www.comscore.com/Insights/Blog/Mobile-Matures-as-the-Cross-Platform-Era-Emerges.

6. *2016 Global Mobile Consumer Survey: US Edition*, Deloitte, https://www2.deloitte.com/us/en/pages/technology-media-and-

Mobile phones have become ingrained in everyday life because of the conveniences that modern mobile technology offers. No longer just a tool that allows for increased telephone communication, smartphones have evolved into personal digital organizers, music players, cameras, email readers, and personal computers. See *Riley v. California*, 134 S. Ct. 2473, 2489 (2014) ("The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."). Cell phones have also supplanted the need for a traditional landline, with many households opting instead for cell phones carried by each family member. Owning a cell phone has become a de-facto requirement for employment of many kinds, and many people are expected, indeed required, to carry a mobile device on their person for a job.

Because of our need and desire to carry cell phones everywhere, we have also come to expect to have service everywhere. Cellular carriers have built and improved their networks to meet this growing need, placing thousands of cell sites throughout our cities, towns, office buildings, hospitals, thoroughfares, and underground subway platforms and tunnels.[7] As demand

---

telecommunications/articles/global-mobile-consumer-survey-us-edition.html (last visited Aug. 11, 2017); Charles Blain, *Police Could Get Your Location Data Without A Warrant. That Has To End*, Wired (Feb. 2, 2017, 7:00 AM), https://www.wired.com/2017/02/police-get-location-data-without-warrant-end/.

7. *Wireless Snapshot 2017*, CTIA (May 2017), https://www.ctia.org/industry-data/ctia-annual-wireless-industry-survey.

has increased, carriers have increased the number of sites and decreased the spacing between sites. These stations allow us to communicate, work, and access information nearly anywhere in the United States. As a consequence, however, they have also allowed cellular carriers to collect increasingly fine-grained information on where we are, what we are doing, and with whom we associate. It is this second consequence—which we view as not widely understood by the public, including many cell phone users themselves—that is the focus of this amicus brief.

B. Cell Phones Constantly Generate Highly Detailed Information On Users' Locations and Movements

Cell phones and other cellular enabled devices allow users to access information about the world—but they also permit others to create a constant, lasting stream of information about those users. One of the key types of information created by our cell phones is CSLI: a record of the location of the cell user in relation to a cell tower, towers, or other cell sites within the network. CSLI is created whenever a cell phone interacts with a cell site. In its simplest version, CSLI is a running record of which cell site a cellphone interacted with, the direction of the cellphone's signal, the date and time of the signal, and, increasingly, the distance of the phone from the cell site.[8]

---

8. Robinson Meyer, *How the Government Surveils Cellphones: A Primer*, The Atlantic (Sept. 11, 2015), https://www.theatlantic.com/technology/archive/2015/09/how-the-government-surveils-cellphones-a-primer/404818/.

As a tracking tool, CSLI has significant advantages over alternative location technology like GPS—including the use of the automatic interaction between the phone and base station, as well as the ability to obtain data in areas where GPS will not function because phones cannot readily receive signals from satellites, such as when underground. CSLI uses features already present in the cellular system infrastructure to pinpoint a device's location. By design, each cell phone within a specified coverage area is within radio range of at least one base station in that carrier's cellular network. Every time a cell phone interacts with a cell site, the cellular provider captures the phone's CSLI—creating a lasting data trail specific to that phone and its user.

1. Law Enforcement Frequently Obtains Both Historic and Real-Time CSLI

Cell providers routinely retain vast amounts of CSLI, and multiple types of reports can be provided or created upon request by law enforcement. These include both historical records and prospective records. Historical location information refers to records collected by the wireless service provider detailing the past location of a cell phone.[9] Prospective location information refers to all cell site information that is disclosed or generated after the government has received court permission to acquire it. This type of request also includes the generation and acquisition of real time location information through a "ping," wherein the provider sends a signal to a phone to determine its location.

---

9. See *In re United States ex. rel. an Order Authorizing the Installation & Use of a Pen Register*, 402 F. Supp. 2d 597, 599 (D. Md. 2005).

Obtaining CSLI, rather than covertly installing a GPS tracking device of the type used in *Jones*[10] (or other similar means), has become an increasingly attractive option for law enforcement to track the location of criminal suspects. AT&T received close to 60,000 requests for historical information in 2015 alone.[11] Similarly, the number of applications under 18 U.S.C. § 2703 for location or internet data (including CSLI) by the U.S. Attorney and the DOJ nearly doubled between 2015 and 2016 and increased over seven-fold between 2013 and 2016 in the Washington, D.C. area.[12] Because cell providers routinely store CSLI during the ordinary course of business, these carriers have the ability to provide law enforcement with vast amounts of data on a handset's precise location at any given time—or over an extended period of time in the past. Cell providers have become potential one-stop shops for the locations and movements of the 95% of Americans who use cell phones.

As law enforcement's appetite for CSLI has grown, the phone companies have created automated self-service websites through which government personnel can request and receive location data.[13] The availability

---

10. *United States v. Jones*, 565 U.S. 400 (2012).

11. Robinson Meyer, *No One Will Save You From Cellphone Tracking*, The Atlantic (June 2, 2016); see also *Transparency Report*, AT&T, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html (last visited Aug. 11, 2017) (most recent data).

12. Russell Brandom, *DC Prosecutors Are Ramping Up Secret Requests for Location and Internet History*, The Verge (July 19, 2017, 1:50 PM), https://www.theverge.com/2017/7/19/15998598/sealed-request-location-internet-history-ip-address-statistics.

13. Letter from Lisa A. Judge, Principal Assistant City Att'y, Tucson Police Dep't to Dan Pochoda, Am. Civil Liberties

of these automated surveillance tools has in turn led to a surge in law enforcement requests that it would have been impossible for phone company personnel to provide.[14] As Judge Kozinski notes, "When requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that 'such dragnet-type law enforcement practices' are already in use." *United States v. Pineda-Moreno*, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, J., dissenting from denial of rehearing en banc).

Union (Sept. 6, 2011), *available at* https://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_tucsonpd_tucsonaz.pdf (describing the location tracking tools offered by AT&T, T-Mobile and Sprint) [hereinafter Tucson Police Dep't Letter]; see also Press Release, AT&T, Information for Public Safety (Sept. 30, 2017) *available at* https://www.al911board.com/sites/default/files/ATT%20Pinging%20and%20NCC%20Info%202013.09.30.pdf (describing AT&T's "locator tool").

14. See Christopher Soghoian, *8 Million Reasons for Real Surveillance Oversight*, Slight Paranoia Blog (Dec. 1, 2009), http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html (quoting Paul Taylor, Electronic Surveillance Manager, Sprint Nextel, speaking on October 2009 panel at ISS World trade show: "We turned it on the web interface for law enforcement about one year ago last month, and we just passed 8 million requests. So there is no way on earth my team could have handled 8 million requests from law enforcement, just for GPS alone. So the tool has just really caught on fire with law enforcement. They also love that it is extremely inexpensive to operate and easy. . .").

C. CSLI is Routinely Collected Without User Knowledge or Consent

This information is routinely collected without the explicit knowledge—or even the active participation—of the phone's user. By design, cell phones generate a constant stream of CSLI, even when the phone is idle. Location tracking through CSLI requires only that a cell phone be on and within range of a cell site. It does not require any affirmative act on the part of the cell phone user.

This fact distinguishes cellular location tracking through CSLI from phone-based GPS tracking, which generally is available only when the phone user *intentionally* runs a location-based application on the phone, or when the target of the tracking carries another device specifically enabled for GPS. The two dominant mobile operating systems, Google's Android and Apple's iOS, explicitly notify the user and request permission before permitting an application to obtain their location information. GPS users therefore have the option of disabling their device's GPS tracking capabilities without interfering with the phone's core functionality. In contrast, the only way for a user to prevent a wireless carrier from generating CSLI records which could later be turned over to law enforcement is for the user to power off their device or put their phone in airplane mode, disabling the phone's cellular, data, and wifi services. Of course, a mobile phone without those services is no longer a mobile phone. It cannot make calls, send messages, access the internet, or be used to communicate with anyone.

D. CSLI is Precise and Becoming More So Every Year

As cellular phones have evolved from simple handsets in the 1980s to powerful handheld personal computers, the precision with which they can be tracked by the network has increased considerably. The latest generation of this technology permits the network to calculate users' locations with a precision that approaches that of GPS.[15] As cellular technology continues to improve, this trend will only accelerate, allowing anyone with access to cell site data to identify the movements of targeted individuals with ever-greater precision.

1. Increases in CSLI Precision Are Being Driven by Continuing Improvements in Network Architecture

The precision of CSLI is a product of two interrelated factors: the density of the cellular network in a given area, and the analytical capabilities of the tracking software employed by the carrier. Both of these factors have increased dramatically since the inception of cellular service in the 1980s, such that CSLI now reveals a user's location with a precision that rivals and in some cases surpasses GPS.[16]

---

15. *Electronic Communications Privacy Act Hearing on ECPA, (Part II): Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. and Investigations of the H. Comm. on the Judiciary*, 113 Cong. 2 (2013) (written statement of Professor Matt Blaze), https://judiciary.house.gov/wp-content/uploads/2016/02/Blaze-Testimony.pdf [hereinafter Blaze].

16. CSLI works inside buildings—which GPS does not—and thus will be able to provide much finer location information in some circumstances than GPS.

The primary factor in determining CSLI precision is the density and location of cellular base stations (sometimes called "sites" or "towers") in the user's immediate area. In a cellular network, base stations are deployed throughout the areas of service such that a cell phone will always be within radio range of at least one base station. This arrangement divides the carrier's coverage area into a mosaic of local "sectors" or "cells," each served by an antenna at a local cellular base station. When a user's phone is connected to the network, the provider can identify the sector in which the phone is located, and, in some cases, further pinpoint the phone's location within a sector.

Over time, these sectors have become much smaller, both to accommodate terrain (as in dense urban areas) and to handle the dramatically increased volume of data transmitted and received by subscribers. As cellular phones have become more popular and as users expect their devices to do more and to work in more locations, the size of the typical cell sector has been steadily shrinking. The Cellular Telecommunications Industry Association (CTIA) recently released a study finding that the number of conventional cell sites increased 57% from 2006 to 2016 (and more than 1000% since 1996).[17] And beyond that, the trend towards smaller cell sectors has been driven by the deployment of the latest generation of micro-scale cellular base stations (called, variously, "microcells", "picocells," and "femtocells").[18] A microcell services a very small

17. *Wireless Snapshot 2017*, CTIA (May 2017), https://www.ctia.org/docs/default-source/default-document-library/ctia-wireless-snapshot.pdf.

18. Joseph Hoy, *Forensic Radio Survey Techniques for Cell Site Analysis* 69 (2015) [hereinafter Hoy].

area, such as the specific floor of a building or individual homes or offices.[19] The number of these small-scale cellular base stations is believed to have exceeded the number of conventional cells in the U.S. as of 2010.[20]

This trend towards an increasingly dense network composed of very small—including building- and room-sized—cells has only accelerated in recent years. Two carriers alone planned to deploy 100,000 small cells in 2016.[21] Relative to conventional cell sites, "the deployment of 100,000 small cells in only one year represents approximately one third of the total number of traditional cell sites deployed over the previous two decades."[22]

---

19. See *United States v. Stimler*, No. 15-4095, 2017 WL 3080866, at *17 (3d Cir. July 7, 2017) (Restrepo, J., concurring in part) (*quoting* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards For Law Enforcement Access To Location Data That Congress Could Enact*, 27 Berkeley Tech. L.J. 117, 132 (2012)) ("Since [2010], wireless network improvements have included the distribution of 'hundreds of thousands of 'microcells,' 'picocells,' and 'femtocells,' which function similarly to hotspots and create CSLI that 'can in some cases be more accurate than GPS.' Even the proliferation of traditional cell towers has resulted in smaller coverage areas and CSLI that is 'far more accurate—in some cases as good as GPS.'").

20. Blaze at 11.

21. Martha DeGrasse, *Can Verizon and AT&T Deploy 100,000 New Small Cells?*, RCR Wireless News (Oct. 29, 2015), http://www.rcrwireless.com/20151029/carriers/can-verizon-and-att-deploy-100000-new-small-cells-tag4.

22. *Enabling the Wireless Networks of Tomorrow*, CTIA (Apr. 2016), https://www.ctia.org/docs/default-source/default-document-library/enabling-the-wireless-networks-of-tomorrow.pdf [hereinafter CTIA, *Enabling the Wireless Networks of Tomorrow*];

Influential policy makers see small cells as a crucial part of the future of cellular telecommunications.[23]

Small cells can even be targeted towards specific public events. For example, at the 2017 Super Bowl, 783 DAS (Distributed Antenna System) antennas were placed strategically throughout the facility, potentially allowing users to be identified as sitting in a particular section of the stadium.[24] Similar systems are also increasingly being deployed to enable cell coverage on public transit routes, such as in the New York City subway system—a feature which will have the collateral effect of allowing CSLI data to identify the locations and movements of public transit customers underground.[25]

By correlating the precise time and angle at which a given device's signal arrives at multiple sector base stations, new technology now makes it practical for a

---

see also *Massive Growth Projected for DAS Deployments*, agl Media Group (Nov. 14, 2013), http://www.aglmediagroup.com/massive-growth-in-u-s-das-deployments-projected-by-igr-research/.

23. Tom Wheeler, Chairman, Fed. Commc'ns Comm'n, Remarks at CTIA Super Mobility Show 2016 (Sept. 7, 2016), *available at* https://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0907/DOC-341138A1.pdf ("[T]here may be millions of small cell sites in the 5G future.").

24. CTIA, *Enabling the Wireless Networks of Tomorrow*, supra note 22.

25. Monica Alleven, *Transit Wireless Wraps Latest Phase of Huge DAS System for NYC Subway Stations*, FierceWireless (Nov. 16, 2015, 9:55 AM), http://www.fiercewireless.com/tech/transit-wireless-wraps-latest-phase-huge-das-system-for-nyc-subway-stations.

network operator to pinpoint a phone's latitude and longitude at a level of accuracy that can approach that of GPS.[26] The increasingly dense configuration of cells has been accompanied by a similarly sharp increase in the richness of the location-tracking data captured by cellular networks. While older-generation cellular networks from the 1980s could only identify the sector a subscriber was in, new technology allows cellular network providers to locate not just the sector in which the user's wireless device is located, but also the distance from the device to the cell site.[27]

Current commercially available versions of this "time-and-angle" location technology can pinpoint a phone's location to an accuracy of within 50 meters or less under many circumstances, and emerging versions of the technology can increase accuracy even beyond that.[28] Crucially, this can be accomplished without requiring any new or special hardware to be installed on users' phones. Users' locations can be tracked with this technology even when no calls are being made or received, as long as their phones are turned on and within a coverage area.

---

26. Blaze at 12.

27. Craig Silliman, Exec. Vice President, Pub. Pol'y & Gen. Counsel, Verizon, *Technology and Shifting Privacy Expectations*, Bloomberg Law (Oct. 7, 2016), https://bol.bna.com/technology-and-shifting-privacy-expectations-perspective/ [hereinafter Silliman].

28. Blaze at 12.

2. The New Generation of Cell Networks Will Allow Increasingly Detailed CSLI

The technical improvements described above have increased the precision of CSLI to a level that would have been unimaginable even a few years ago. Today, in many circumstances, CSLI is effectively as accurate as GPS. Depending on the density of cell base stations in an area, CSLI can now often pinpoint an individual device to particular building, or even a specific room within a building.[29] This change is perhaps particularly applicable to users in urban areas, where many individual businesses, hospitals, subway systems, and other facilities have now installed dedicated micro-cells—allowing CSLI to pinpoint individuals at these locations.[30] In the past, when cell sectors were widely spaced and before the availability of the enhanced network-based location technologies now being deployed by wireless carriers, it may have been technically sound to make a distinction between location based on the cellular network (at presumably low accuracy) and that based on GPS (at higher accuracy). Today, however, this distinction is increasingly obsolete.

---

29. Blaze at 11–12.

30. To a significant degree, this increase in precision is being driven by government objectives relating to the provision of emergency services. See Brian Fung, *New FCC Proposal Would Require Pinpoint Location Accuracy for 911 Calls*, Washington Post (Feb. 20, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/02/20/new-fcc-proposal-would-require-pinpoint-location-accuracy-for-911-calls/ ("The Federal Communications Commission wants to mandate that within 30 seconds of a call, 911 dispatchers will be able to pinpoint a caller's location to within 50 meters on the correct floor. The FCC hopes that by the end of five years, 80 percent of all wireless 911 calls will benefit from the capability.").

Although CSLI precision varies based on a number of factors, its precision is highly dynamic and, at any given time, hard to predict. As individuals move around an area, the precision of CSLI data will vary widely for any given customer over the course of a given day, from the relatively less precise to the relatively very precise, and neither the user nor the carrier will be able to predict whether the next data location collected will be relatively more or less precise. This is a significant change from the introduction of cellphones in the 1980s, when CSLI could only provide an approximate location over a wide geographic area.[31]

Even imprecise CSLI can still be mined to reveal a user's location with high precision. Analytical software can track an individual as they move and reconstruct their path with a high degree of accuracy.[32] Every time an individual crosses a boundary between two cell sites, a record is created of their movement.[33] In dense urban areas or while driving, such handoffs can happen very

---

31. At trial, the government's expert, Agent Hess, testified that within a city such as Detroit, a cell site's coverage area typically would extend "a-half mile to two miles." J.A. 47. This testimony appears to refer to the maximum potential size of a cell. Today, in urban areas, cell site coverage areas are often smaller, with cell sites as close as a few hundred meters apart. Hoy at 244. Those coverage areas will almost inevitably continue to shrink as small cell sites are added to keep pace with the demands of coverage and capacity.

32. Conference Report, Arvind Thiagarajan et. al., *Accurate, Low-Energy Trajectory Mapping for Mobile Devices*, NSDI'11 Proc. of the 8th USENIX Conference on Networked Sys. Design and Implementation (Mar. 30, 2011), *available at* http://db.csail.mit.edu/pubs/ctrack-cr.pdf.

33. Blaze at 9–10.

frequently—often, several times per minute. If a user moves from one sector to another at a particular time, a CSLI viewer can infer that the user was on the sector boundary at that time. By superimposing the boundary onto a map, the viewer can narrow the location down further to places on the boundary on which a person is able to walk or drive. And by aggregating boundary-crossing information over time, the viewer can determine whether the user is walking or driving, and at roughly what speed, which in turn allows additional inferences regarding location (e.g., highway vs. side street vs. rail corridor).

That is not all, as a striking 2012 study demonstrated. That study, which used a data set of coarse location data from a mobile phone operator from April 2006 to June 2007, demonstrated that not only can an accurate location path be reconstructed from CSLI, but also that knowing just four *random* data points of a user's CSLI was sufficient to uniquely identify 95% of the users of the mobile phone operator.[34] In this way, CSLI can be used to effectively "fingerprint" individuals based on their patterns of movement. Given the increased precision of CSLI and other technological advances since 2012, a similar study today would only more powerfully demonstrate what can be learned from our locations and movements.

The increase in CSLI precision is the result of socially desirable progress, namely the increasing coverage, speeds, and reliability of cellular service networks.

---

34. Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Scientific Reports 3 (Mar. 25, 2013), https://www.nature.com/articles/srep01376.pdf [hereinafter de Montjoye et al., *Unique in the Crowd*].

However, as discussed below, these improvements come at a high potential cost to privacy. As the Court considers this case, it should resist creating any new Fourth Amendment rule based on the assumption that the location data created by CSLI is relatively crude or minimally revealing, as it was in the 1980s. In fact, the opposite is true: CSLI has become highly revealing in the areas in which most Americans live, and will only become more so going forward.

3. Carriers Are Storing Increasingly Large Amounts of CSLI and Analyzing this Data Is Increasingly Easy

As storage costs have fallen, and as network management tools have become more sophisticated and data-intensive, cellular carriers have begun generating, storing, and retaining increasingly vast amounts of customer CSLI.[35] Even as long ago as 2011, it was estimated that "[t]he information identifying the location of each of one million people to [an accuracy of about 15 feet] at 5-minute intervals, 24 hours a day for a full year could easily be stored in 1,000 gigabytes, which would cost slightly over $50."[36] Given current trends, one can

35. See *Cell Phone Location Tracking Request Response - Cell Phone Company Data Retention Chart*, Am. Civil Liberties Union, *available at* https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart (last visited Aug. 11, 2017); see also Silliman ("[O]ur network now collects more voluminous and more precise location information than [2010 and 2011]").

36. John Villasenor, *Recording Everything: Digital Storage as an Enabler of Authoritarian Governments*, Brookings 4 (Dec. 14, 2011), https://www.brookings.edu/wp-content/uploads/2016/06/1214_digital_storage_villasenor.pdf.

safely anticipate that the cost of storage will continue to fall and the amount of data stored will continue to grow in the future.

Meanwhile, retained CSLI has become increasingly useful for network management; for example, having access to historical CSLI allows cellular service providers to know which cell sites receive the most traffic, and where additional cell sites should be placed to most efficiently serve their customers.[37] Carriers have also found commercial uses for location data, allowing them to profit from the retention of data.[38] Importantly, the capability of the third-party analytical tools used by wireless carriers has rapidly improved, with newer "mass location" technology from firms such as Polaris Wireless giving carriers the ability to use historical CSLI to accurately reconstruct the locations of *all* users who were connected to their network at a given time.[39] These systems, which are marketed to carriers as ways to streamline their networks and improve their ability to respond to emergencies, have potentially significant implications for the quality and precision of historical CSLI available to

---

37. Blaze at 15.

38. Kate Kaye, *The $24 Billion Dollar Business That Telcos Don't Want to Talk About*, Advertising Age (Oct. 26, 2015), http://adage.com/article/datadriven-marketing/24-billion-data-business-telcos-discuss/301058/.

39. Conference Presentation, Mahesh Patel, *Location for Public Safety and Emergency Management*, Geo Smart Asia 2016 (Oct. 18, 2016), http://geosmartasia.org/presentation/location-intelligence-for-public-safety-and-emergency-management.pdf.

law enforcement.[40] Such tools significantly amplify the accuracy of the underlying CSLI data, which, as noted above, is itself becoming more accurate over time.

Because cellular service providers retain such lengthy periods of historical CSLI data, the government is often able to request (and obtain) access to data vastly in excess of what would be provided under a traditional search warrant limited by probable cause.[41] Recent cases considered by the circuit courts have borne this out. In this case, the government obtained 127 days' worth of CSLI for Timothy Carpenter and 88 days for Timothy Sanders. Pet. App. 5a. In another recent case, the government obtained 221 days' worth (over 28,000 location data points) of CSLI for two other suspects. *United States v. Graham*, 824 F.3d 421, 446 (4th Cir. 2016) (Wynn, J. dissenting). All of that data was obtained, of course, without a warrant.

In each of these cases, had traditional methods of surveillance been utilized to collect the same amount of information, the cost to the government would have run into the hundreds of thousands of dollars for each individual surveilled.[42] For example, while foot pursuit

---

40. Bhavin Shah, *Polaris Wireless Solutions*, Law and Order Mag. (July 2013), http://www.hendonpub.com/law_and_order/articles/2013/07/polaris_wireless_location_solutions.

41. See No. 16-402 Pet. Br. 56–58, (discussing that the orders used to obtain CSLI in this case lacked particularity).

42. Kevin Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones*, 123 Yale L.J. Online 335, 350 (2014), http://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones [hereinafter Bankston & Soltani].

of a subject has been estimated to cost over $30,000 for 28 days of surveillance, the same location data insight can be gathered by acquiring CSLI from cellular service providers for a tiny fraction of that cost.[43] Reconstructing a suspect's past movements over a period of months through canvass interviews and other historical sources would almost certainly have been even more expensive and time-consuming. While some carriers charge law enforcement a small fee to recoup the costs of producing CSLI reports, that fee is miniscule in comparison to the expense of traditional methods of surveillance,[44] allowing the government to conduct more invasive surveillance more indiscriminately than ever before. *Jones*, 565 U.S. at 415–416 (Sotomayor, J., concurring) ("[B]ecause GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" (quoting *Illinois v. Lidster*, 540 U.S. 419, 426 (2004))); *Jones*, 565 U.S. at 429 (2012) (Alito, J., concurring in the judgment) ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly . . . . Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap."); cf. *United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007) ("The new technologies enable, as the old (because of expense) do not, wholesale surveillance.").

---

43. *Id.*

44. Tucson Police Dep't Letter; Bankston & Soltani at 341–350.

In addition to being relatively cheap to obtain and store, CSLI data is uniquely easy to analyze in bulk as compared to previous forms of surveillance data, such as wiretaps. Chiefly, this is because CSLI is *structured data*. That is, the information is stored in a predictable and standardized format that computers can be easily programmed to read, interpret, and even analyze, all without the need for human involvement.

A market has already developed for vendors who assist law enforcement in managing and analyzing CSLI. A number of turn-key solutions—most notably Palantir, IBM Analyst's Notebook, and Pen-Link—exist for law enforcement and other government entities to ingest cellular surveillance data directly from the wireless carriers' computer systems and convert raw CSLI data into a format suitable for easy review by investigators.[45] These analytic software tools allow anyone with CSLI

---

45. See *Unique Features of Pen-Link v8*, Pen-Link 4–5 (Apr. 17, 2008) ("Pen-Link offers a suite of powerful 'special' functions to help the intelligence analyst perform necessary and common analytical tasks that, when performed with traditional methods, can become tedious, error prone, and extremely time-consuming."), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/1282888/09-07-14-2009-pen-link-software-sole-source.pdf (describing the capability to import 170 different data formats, used by phone companies to provide call detail records); see also *Cellular Analysis Mapping Program v2.7*, Officer.com, http://www.officer.com/product/10855725/cellular-mapping-cellular-analysis-mapping-program-v27 (last visited Aug. 11, 2017); GeoTime, https://geotime.com (last visited Aug. 11, 2017); Mark Harris, *How Peter Thiel's Secret Company Secretive Data Company Pushed Into Policing*, Wired (Aug. 9, 2017) https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/ (discussing increased use of Palantir technology by law enforcement).

to quickly and easily derive personally identifying information—including a targeted individual's movements, relationships, and private associations. Indeed, AT&T now offers a premium surveillance service to law enforcement agencies in which the company mines 26-years' worth of subscriber records, including location data, to allow agencies to look for patterns related to specific targets.[46]

II. CELL SITE LOCATION INFORMATION REVEALS AN EXTRAORDINARILY DETAILED PICTURE OF AN INDIVIDUAL'S LIFE, EVERY BIT AS REVEALING AS THE CONTENT OF THEIR COMMUNICATIONS

A. Even Discrete Pieces of CSLI Reveal Extremely Sensitive Information

As explained above, the volume, ubiquity, and structured nature of CSLI makes the privacy and expressive implications of government access to this data unique. Even a limited amount of CSLI data can be used to reveal sensitive, detailed information about individuals. This is true because of two important facts about CSLI location tracking.

---

46. See Kenneth Lipp, *AT&T is Spying on Americans for Profit*, Daily Beast (Oct. 25, 2016, 1:13 AM), http://www.thedailybeast.com/atandt-is-spying-on-americans-for-profit (describing the extensive use of AT&T's Hemisphere system by law enforcement agencies); see also Scott Shane and Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, N.Y. Times (Sept. 1, 2013) ("Some four billion call records are added to the database every day . . . ."), *available at* http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html.

First, most people carry their cell phone on or very near their bodies for the majority of the day, and so CSLI tracking is *personal*. In other words, any given data point of CSLI is highly likely to correspond to the precise location of an individual. This contrasts with other surveillance technologies, such as GPS devices attached to cars, which generally remain on roads, in driveways, or in garages. In contrast, the majority of individuals carry their phones on their person or within several feet the majority of the time.[47] This means that CSLI allows the government to track individuals, not just cars, and through private spaces, not just public ones. The government can collect a detailed record of the person's movements through the world, no matter how he or she chooses to travel, even recording movements through a particular building when that building contains multiple microcells.[48] In short, CSLI allows the government to track individuals not only through places where it would

---

47. See Chelsea J. Carter, *Where (and When) Do You Use Your Smartphone: Bedroom? Church?*, CNN (July 13, 2013, 9:46 PM), http://www.cnn.com/2013/07/13/tech/smartphone-use-survey/.

48. E.g., Brassil et al., *Authenticating Location with Femtocells*, Mass. Inst. Tech., http://web.mit.edu/ravinet/www/femto-v0.8%5B1%5D.pdf (last visited Aug. 11, 2017) ("Despite their limited wireless range (e.g., tens of meters), femtocells meet the various regulatory, compliance and spectrum use requirements of cellular base stations, including supporting location service."); Gavin Horn, *3GPP Femtocells: Architecture and Protocols*, Qualcomm 59 (Sept. 2010), https://www.qualcomm.com/media/documents/files/3gpp-femtocells-architecture-and-protocols.pdf; *Products: Femtocells*, Nokia, https://networks.nokia.com/products/femtocells (last visited Aug. 11, 2017) (describing Nokia's femtocell offering and noting that "more than 80 percent of mobile usage occurs inside buildings").

otherwise be uneconomical to do so, but even through places where it would otherwise be effectively *impossible* for the government to do so, such as within the surveillance target's own home or office.

Second, because of the increasing precision of CSLI (discussed above in Section I), even a single data point has the potential to reveal highly sensitive information about a person's associations, habits, beliefs, medical conditions, and vices. This is because of the common sense observation that individuals often go to *particular locations* for *particular purposes*. If an individual's CSLI record contains one or more data points corresponding to a certain church, the individual's religious beliefs can be inferred.[49] If an individual's CSLI record contains a data point corresponding to the time and place of a political rally or protest, the individual's political views can similarly be known or predicted.

The government could also learn, through CSLI, information and relationships generally held as confidential. Imagine, for instance, a surveillance target's CSLI data containing one or more contacts in the cell site coverage area containing the office of a prominent divorce lawyer, or a lawyer specializing in whistleblower suits. Without knowing anything about the contents of the communications of the surveillance target, the government could predict the surveillance target's personal life and protected associations.

---

49. As the ACLU noted in its brief before the Sixth Circuit, petitioner's own CSLI did in fact reveal that he attended a particular church in Detroit nearly every Sunday. See Brief of Amicus Curiae Am. Civil Liberties Union et al. at 11, 819 F.3d 880 (2016) (Nos. 14-1572 & 14-1805), *available at* https://www.aclu.org/legal-document/united-states-v-carpenter-amicus-brief.

Similarly, sensitive medical information about individuals could be determined by monitoring CSLI. Given the high and growing precision of CSLI data in urban areas, a surveillance target's CSLI could reveal with a high degree of confidence that the target visited an oncologist, a plastic surgeon, a psychiatrist, an addiction rehabilitation facility, or an abortion clinic.[50] Even a single contact in the cell site coverage areas containing one of these facilities could enable a prediction about the medical needs of the surveillance target. More frequent contacts would simply verify and increase the government's certainty about the medical condition of the target.

More revealing inferences can be drawn by combining CSLI with additional information (including public information) about the surveillance target. For instance, if the target is widely known as a mergers and acquisitions specialist and the target visits both the offices of a startup and the campus of a larger company, it could be inferred that the purchase of the startup may be in the works. If the target is a government employee and the target visits the offices of a newspaper prior to the publication of a story revealing government malfeasance, the government would similarly be able to infer the source of the story.

---

50. In one particularly striking example, advertisers sought to use mobile device location history to target pro-life messages to women who had recently visited abortion clinics—a practice that was ultimately prohibited by the Massachusetts Attorney General. See Press Release, Office of the Mass. Attorney General, AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities (Apr. 4, 2017), http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-04-04-copley-advertising-geofencing.html.

Because each CSLI location data point also includes a timestamp,[51] an individual data point has the potential to convey even more detailed or nuanced information. For example, churches and community centers frequently offer different programs at different times of the day and on different days of the week. CSLI data showing that a surveillance target visited a church at 10:00 am on Sunday morning could lead to an inference of religious observance; CSLI showing that the target visited that same church at 8:30 pm on Thursday, when an Alcoholics Anonymous meeting is scheduled to take place, could lead to a very different inference.[52] The same is true of scheduled lectures at community centers or universities, movie showtimes, or political rallies.

Accordingly, it is no exaggeration to say that, by obtaining and analyzing the CSLI of an individual's cellular device, the government can gain "a clear picture of a person's habits and preferences, and indeed, of his or her life."[53] As the D.C. Circuit recognized, "[a] person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular

---

51. Time is metadata that is also included with CSLI. See, e.g., J.A. 135–136.

52. E.g., *Events Calendar*, Lutheran Church of the Reformation, https://www.reformationdc.org/events-calendar (last visited Aug. 11, 2017).

53. Kai Biermann, *Betrayed By Our Own Data*, Zeit Online (Mar. 10, 2011, 5:09 PM), http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz [hereinafter Biermann].

individuals or political groups—and not just one such fact about a person, but all such facts." *United States v. Maynard*, 615 F.3d 544, 561–62 (D.C. Cir. 2010); see also *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."). And, as discussed in above, this information has become vastly more detailed and precise since the dawn of the cellular telephone, and will only become more so in the years to come.

B. Aggregated CSLI Has the Potential to Reveal Even More Sensitive Detail

While even a single data point of CSLI can be highly revealing of the intimate details of a person's life, the level of insight deepens when CSLI data is *aggregated*, spanning days, months, or even years.

Many, if not most, adults in the United States have a fairly consistent travel pattern on a day-to-day and week-to-week basis. As studies have recognized, the cell sites that are most often contacted by the typical user are those that serve the user's home and the user's place of employment.[54] However, when a user departs from those two cell site coverage areas, or varies their usual pattern, even more personal information about their activities can become apparent.

A striking example is provided by the case of Malte Spitz, a German politician. In 2009, Mr. Spitz sued his

54. de Montjoye et al., *Unique in the Crowd* at 4.

cellular service provider, Deutsche Telekom, to obtain the records that it kept on his cellular device, including CSLI.[55] He obtained six months of data, from August 2009 to February 2010, representing over 35,000 individual data points.[56] Mr. Spitz, *Die Zeit*, and OpenDataCity assembled the data into a nearly complete record of Mr. Spitz's life during these six months[57] As the German newspaper *Die Zeit* noted in reporting on the story and visualizing the data, "By pushing the play button, you will set off on a trip through Malte Spitz's life,"[58] including his movements, his family life, and all of his work and recreation activities. Given that the analysis of Mr. Spitz relied on 2011 tools and 2009–2010 CSLI data, a similar analysis conducted by law enforcement using the tools and data available today would inevitably be even more revealing.

As *Die Zeit*'s analysis of Mr. Spitz's CSLI noted, aggregated CSLI "reveals when Spitz walked down the street, when he took a train, when he was in an airplane. It shows where he was in the cities he visited. It shows when

---

55. Interview by Cyrus Farivar with Malte Spitz (Jan. 4, 2011), *available at* http://p.dw.com/p/10m0A; Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. Times (Mar. 26, 2011), *available at* http://www.nytimes.com/2011/03/26/business/media/26privacy.html [hereinafter Cohen].

56. Cohen, supra note 55.

57. *Tell-all Telephone*, Zeit Online (Mar. 2011), http://www.zeit.de/datenschutz/malte-spitz-data-retention [hereinafter Tell-all Telephone].

58. Id.; see also *Data Retention in Switzerland*, Digitale Gesellschaft, https://www.digitale-gesellschaft.ch/vds-suisse/index_en.html (last visited Aug. 11, 2017) (similar data for the Swedish politician Balthasar Glättli).

he worked and when he slept, when he could be reached by phone and when he was unavailable. It shows when he preferred to talk on his phone and when he preferred to send a text message. It shows which beer gardens he liked to visit in his free time. All in all, it reveals an entire life."[59]

An interactive map provided by Die Zeit demonstrates the accuracy and richness of the CSLI data retained by Deutsche Telekom:[60]

Aggregation over time may even enable social profiling of surveillance targets. A study by researchers at MIT, Harvard, and Ecole Normale Supérieure de Lyon suggests that automated analysis of a person's CSLI records can lead to inferences about key aspects of their personality.[61]

---

59. Biermann, supra note 53.

60. *Tell-all Telephone,* supra note 57.

61. Yves-Alexandre de Montjoye et al., *Predicting Personality Using Novel Mobile*

Knowing the total distance traveled per day and the places visited by that participant, researchers could guess with statistically significant accuracy whether the participant rated low, average, or high for neuroticism, defined as their tendency to experience strong negative emotions.[62] Although research like this is undoubtedly speculative, the study provides insight into the types of inferences that may become possible when an investigator has access to the quantities of aggregated CSLI data often available to law enforcement today.

Beyond what it can reveal about an individual, aggregated CSLI data can permit the government to draw connections between people, including individuals who were not the intended target of surveillance. In one study, friendships between two individuals could be inferred with *greater than 95% accuracy* based only on how frequently those two people were co-located outside the workplace and on evenings and weekends.[63]

Once the place and purpose of a meeting has been identified through CSLI, it is trivial for other associational

---

Phone-Based Metrics, *in* Social Computing, Behavioral-Cultural Modeling and Prediction 48, 49 (A.M. Greenburg et al. eds, 2013) (ebook) *available at* https://pdfs.semanticscholar.org/6b7c/d082d71e97bb0dd8f51304e93b83b8178cc3.pdf.

62. Location information is just one type of metadata analyzed in this study that can be used to predict personality traits of individuals.

63. Nathan Eagle et al., *Inferring Friendship Network Structure by Using Mobile Phone Data*, 106-36 Proc. of the Nat'l Acad. of Sci. 15274, 15275 (Sept. 8, 2009), http://www.pnas.org/content/106/36/15274.full.pdf.

links to be drawn. For example, if law enforcement has followed the CSLI trail of a surveillance target to a Thursday, 8:30 pm Alcoholics Anonymous meeting, requesting a tower dump of the cell site serving that particular location at that particular time will reveal all the devices—and therefore individuals—in that meeting. Obtaining tower dumps of that cell site at that day and time across several weeks could permit law enforcement to uncover the repeat attendees of such a meeting. Observing whether one or more of the devices of those other repeat attendees appear in the same cell site as the surveillance target outside of the hours of the Alcoholics Anonymous meeting could permit investigators to identify persons that the target is particularly friendly with, including, for example, the target's sponsors. The same conclusions hold for other sensitive and protected associational activities—including religious evangelism, student activism, and union organizing.

* * *

The unique power—and danger—of CSLI underscores the need for care in fashioning the legal rules that govern its access. In an age of ubiquitous cell phone use, CSLI can reveal nearly everything about a person's life. Unrestricted law enforcement access to this data allows the government to reconstruct the detailed movements, personal activities, habits, relationships, and associations not just of the direct targets of its surveillance but of third parties as well. Given the sensitivity of this information and the potential for its misuse—factors that will only increase over time—the Court should make clear that the government needs to obtain a warrant before being permitted to obtain and use CSLI.

CONCLUSION

The judgment of the Court of Appeals should be reversed.

Respectfully submitted,

ALEX ABDO
Counsel of Record
JAMEEL JAFFER
KNIGHT FIRST AMENDMENT INSTITUTE
AT COLUMBIA UNIVERSITY
535 West 116th Street
314 Low Library
New York, NY 10027
(212) 854-9600
alex.abdo@knightcolumbia.org

BRIAN WILLEN
JACK MELLYN
SAMUEL DIPPO
WILSON SONSINI GOODRICH & ROSATI
1700 K Street NW
Washington, DC 20002
(202) 973-8800

Counsel for Amici Curiae

RECORD AND BRIEF

Supreme Court, U.S.
FILED
AUG 14 2017
OFFICE OF THE CLERK

No. 16-402

IN THE
Supreme Court of the United States

TIMOTHY IVORY CARPENTER, *Petitioner*,
v.
UNITED STATES OF AMERICA, *Respondent*.

On Writ of Certiorari
to the United States Court of Appeals
for the Sixth Circuit

Brief *Amicus Curiae* of United States Justice Foundation, Gun Owners Foundation, Gun Owners of America, Inc., Citizens United, Citizens United Foundation, Downsize DC Foundation, DownsizeDC.org, Conservative Legal Defense and Education Fund, The Heller Foundation, and Policy Analysis Center in Support of Petitioner

JOSEPH W. MILLER
Attorney for Amicus Curiae
U.S. Justice Foundation

MICHAEL BOOS
Attorney for Amici Curiae
Citizens United and
Citizens United Foundation

J. MARK BREWER
Attorney for Amicus Curiae
Conservative Legal Defense
and Education Fund

ROBERT J. OLSON*
HERBERT W. TITUS
WILLIAM J. OLSON
JEREMIAH L. MORGAN
WILLIAM J. OLSON, P.C.
370 Maple Ave. W., Ste. 4
Vienna, VA 22180-5615
(703) 356-5070
wjo@mindspring.com
Attorneys for Amici Curiae

**Counsel of Record*
August 14, 2017

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES iii

INTEREST OF THE *AMICI CURIAE* 1

SUMMARY OF ARGUMENT 2

ARGUMENT

I. The Court below Erroneously Utilized Privacy Instead of Property as the Fourth Amendment Baseline 5

A. United States v. Jones Restored the Fourth Amendment Property Principle . . . 5

B. The Sixth Circuit Elevated the Judicially Created Privacy Test Over the Fourth Amendment's Property Principles 8

II. The Warrantless Search Violated Defendants' Fourth Amendment Property Rights in Their Persons 11

III. The Warrantless Search of the CSLI Data Violated Defendants' Fourth Amendment Property Rights in Their Papers and Effects . 15

IV. The Government Scheme of Broadcast Regulation Has Conditioned One's Full Participation in Modern Society upon Forfeiture of Fourth Amendment Rights 21

A. The FCC Pervasively Regulates the Cellular Spectrum. 23

B. Contrary to the Government Claim, the Cellular Network Is "Large Enough to Accommodate Everybody" 28

C. The FCC Has Made Cellular Providers Necessary and Helps Them Protect Their Turf from Competing Technologies 31

D. CSLI Is Not "Voluntarily Conveyed" to Wireless Providers, But Is Mandated by Government 33

E. CSLI Records Are Required by the Government 35

F. Summary 36

CONCLUSION 37

TABLE OF AUTHORITIES

Page

HOLY BIBLE
Exodus 20:15 18
Exodus 20:17 18
Exodus 22:3 18
Leviticus 19:13 18
I Samuel 8:10-22 18
Proverbs 30:8-9 18
Mark 10:19 18

CONSTITUTION
Amendment IV ..... 2, *passim*

STATUTE
47 U.S.C. § 222 33
Communications Act of 1934, Pub. L. No. 73-416 23
Pub. L. No. 106-81 34

CASES
ABC, Inc. v. Aereo, Inc., 134 S.Ct. 2498 (2014) ... 22
CBS v. Democratic Nat'l Committee, 412 U.S. 94 (1973) 22, 26
District of Columbia v. Heller, 554 U.S. 570 (2008) 15
Entick v. Carrington, 95 Eng. Rep. 807 (C.P. 1765) 6, 11
Ex parte Jackson, 96 U.S. 727 (1878) 17
Florida v. Jardines, 133 S.Ct. 1409 (2013) . 2, *passim*
Katz v. United States, 389 U.S. 347 (1967) 2, 6
National Broadcasting Co. v. United States, 319 U.S. 190 (1943) 24, 25

Red Lion Broadcasting Co. v. FCC, 395 U.S. 89 (1969) 25
Riley v. California, 134 S.Ct. 2473 (2014) .. 3, *passim*
Smith v. Maryland, 442 U.S. 735 (1979) ... 9, 17, 35
United States v. Jones, 565 U.S. 400 (2012) ..... 2, *passim*

MISCELLANEOUS

B. Bailyn, The Ideological Origins of the American Revolution (Cambridge, Mass, 1967) 13
W. Blackstone, Commentaries on the Laws of England 7, 11
J. Cribbett, Principles of the Law of Property (Foundation Press, 2d edition:1975) 15
E. Falcon, "FCC Helped Create the Stingray Problem, Now it Needs to Fix It," Electronic Frontier Foundation (Oct. 6, 2016) 32
Dorothy J. Glancy, "The Invention of the Right to Privacy," 21 ARIZ. L. REV. 1 (1979) 6
D. Goldman, "Sorry, America: Your wireless airwaves are full," CNN Money (Feb. 21, 2012) 28
M. Lasar, "How the Titanic disaster pushed Uncle Sam to 'rule the air,'" ARS Technica (Jul. 7, 2011) 23
C. Lecher, "How the FCC's massive airwaves auction will change America — and your phone service," The Verge (Apr. 21, 2016) ... 27
L. Levison, "Secrets, lies and Snowden's email: Why I was forced to shut down Lavabit," *The Guardian* (May 20, 2014) 19
J. Locke, Two Treatises of Government 13
C. Oakes, "'E911' Turns Cell Phones into Tracking Devices," Wired Magazine (Jan. 6 , 1998) ... 33

D. Quick, "No mobile phone coverage? No worries, researchers put a tower in a phone," New Atlas (Jul 12, 2010) 31
J. Rakove, Revolutionaries: A New History of the Invention of America (Houghton Mifflin Harcourt: 2010) 13
A. Rand, "The Property Status of Airwaves," The Objectivist Newsletter, vol. 3, no. 4, p. 1 (Apr. 1964) 25, 26
D. Shepardson, "FCC spectrum auction bidding ends at $19.6 billion," Reuters (Feb. 10, 2017) 28
T. Simonite, "Future Smartphones Won't Need Cell Towers to Connect," MIT Technology Review (Sep. 29, 2014) 32
H. Titus & W. Olson, "*United States v. Jones*: Reviving the Property Foundation of the Fourth Amendment," CASE WESTERN RESERVE J. OF LAW, TECHNOLOGY & THE INTERNET, vol. 3, no. 2 (Spring 2012) 7
S.D. Warren and L.D. Brandeis, "The Right to Privacy," HARV. L.REV., vol. IV, no. 5 (Dec. 15, 1890) 5, 16
N. Webster, American Dictionary of the English Language (1828) 12

INTEREST OF THE *AMICI CURIAE*[1]

U.S. Justice Foundation, Gun Owners Foundation, Citizens United Foundation, Downsize DC Foundation, Conservative Legal Defense and Education Fund, The Heller Foundation, and Policy Analysis Center are nonprofit educational organizations, exempt from federal income tax under section 501(c)(3) of the Internal Revenue Code ("IRC"). Gun Owners of America, Inc., Citizens United, and DownsizeDC.org are nonprofit social welfare organizations, exempt from federal income tax under IRC section 501(c)(4).

These legal and policy educational organizations were established, *inter alia*, for purposes related to participation in the public policy process, which purposes include programs to conduct research and to inform and educate the public on the proper construction of state and federal constitutions, as well as statutes related to the rights of citizens, and questions related to human and civil rights secured by law. Many of these *amici* also filed *amicus* briefs in other Fourth Amendment cases involving cell site location information ("CSLI"), including two briefs in United States v. Graham, and one in United States v. Zodhiates:

- United States v. Graham, U.S. Court of Appeals for the Fourth Circuit (Jan. 22, 2016) (Brief *amicus curiae* of DownsizeDC.org, *et al.*).

---

[1] It is hereby certified that counsel for the parties have consented to the filing of this brief; that no counsel for a party authored this brief in whole or in part; and that no person other than these *amici curiae*, their members, or their counsel made a monetary contribution to its preparation or submission.

- Graham v. United States, U.S. Supreme Court (Nov. 3, 2016) (Brief *amicus curiae* of U.S. Justice Foundation, *et al.*).

- United States v. Zodhiates, U.S. Court of Appeals for the Second Circuit (July 5, 2017) (Brief *amicus curiae* of Downsize DC Foundation, *et al.*).

Additionally, these *amici* filed *amicus* briefs in the U.S. Supreme Court in United States v. Jones, 132 S.Ct. 945 (2012), at both the petition stage and the merits stage:

- Brief *Amicus Curiae* of Gun Owners of America, Inc., *et al.* in Support of Neither Party, On Petition for Writ of Certiorari (May 16, 2011).

- Brief *Amicus Curiae* of Gun Owners of America, *et al.*, in Support of Respondent, On Writ of Certiorari (Oct. 3, 2011).

SUMMARY OF ARGUMENT

The decision of the Sixth Circuit demonstrates once again that old habits die hard. Despite this Court's clear and unambiguous revitalization of the textual and historic property basis of the Fourth Amendment in United States v. Jones, and again in Florida v. Jardines, the Sixth Circuit fell back upon the familiar "reasonable expectation of property" created out of whole cloth in Katz v. United States. Inverting this Court's two-step process to evaluate

Fourth Amendment challenges, the court below failed to properly evaluate whether defendants had a property interest in its CSLI, and concluded only that they had no protected privacy interest.

Had the court below conducted a proper analysis, it would have found that defendants had two types of interests that are protected from Fourth Amendment searches and seizures. First, the warrantless search of their CSLI violated the defendants' property right in their persons. At the time of the ratification of the Fourth Amendment, it was generally understood that each person had a protected property interest not just in the things he owned, but first, as the Fourth Amendment text makes clear, in his "person." As made clear by giants like Blackstone and Locke, his right to his person encompassed his right to the labor of his body, his freedom of movement, and his right to communicate with and interact with others.

Second, the warrantless search of defendants' CSLI intruded on protected "papers" and "effects," especially when that data revealed to the government what this Court in Riley v. California described as "the privacies of life." That location data was of the same nature as, even though somewhat less precise than, the GPS data collected about Antoine Jones, deemed to be protected by this Court in 2008. It makes no difference whatsoever that this information did not include the "content" of those communications, for disclosure of location data clearly chills associational and expressive freedoms, in addition to violating the Fourth Amendment.

Lastly, as both this Court and Petitioner's brief have noted, cellular phones have become integral and indispensable to full participation in American society. The government contends that defendants' transmission of CSLI was "voluntary," and its collection by cell phone providers was for the "business purposes" of their cellular providers. However, the government certainly cannot rely on supposed voluntary submission of data to a cell phone provider when it was the federal government that designed the very system of cell phone use that now exists. For nearly a century, the Federal Communications Commission has been given, and exercised, sweeping powers over the nation's airwaves, designating various radio frequencies for specific uses by specific users. Justice Douglas famously described the airwaves as "the common heritage of all the people," yet the FCC has sold cellular frequencies to the cellular providers, and prohibited Americans from using them unless via those government gatekeepers. Now, rather than those frequencies being freely accessible by "all the people," Americans instead must deal with the cellular companies who control them, and the FCC protects these monopolies from competing and emerging technologies. What's more, it was Congress that initially made the push for the creation of location information, and required cellular companies to collect it under certain circumstances.

Indeed, in order to communicate in today's modern world, defendants were forced onto government-controlled airwaves, on a government-approved cellular network, using government-mandated technology, transmitting government-

required location data. Under such a system of pervasive control, the Orwellian tracking of Americans cannot be justified on a theory which presumes voluntary action and consent. Legalization of constitutional violations does not make them constitutional.

ARGUMENT

I. THE COURT BELOW ERRONEOUSLY UTILIZED PRIVACY INSTEAD OF PROPERTY AS THE FOURTH AMENDMENT BASELINE.

A. United States v. Jones Restored the Fourth Amendment Property Principle.

As advocates and judges, we would do well to remind ourselves that the Fourth Amendment guarantee of "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" was written and ratified in the days of Sir William Blackstone's Commentaries on the Laws of England, a century before Louis D. Brandeis' celebrated Harvard Law Review essay on "The Right to Privacy"[2] was published. In Blackstone's time, as this Court recognized in United States v. Jones, 565 U.S. 400 (2012), the common law backdrop to the Fourth Amendment was Lord Camden's declaration in the 1765 case of Entick v. Carrington that "our law holds

---

[2] S.D. Warren and L.D. Brandeis, "The Right to Privacy," HARV. L.REV., vol. IV, no. 5 (Dec. 15, 1890).

the property of every man [to be] sacred." *Id.* at 95 Eng. Rep. 807, 817 (C.P. 1765). Yet, as Justice Scalia observed in Jones, in the 21st century, the Fourth Amendment's "close connection to property" was in danger of being overrun by a judicially invented test connecting the Amendment only to "privacy," not property. *Id.* at 405-08.

Indeed, birthed by this Court in 1967 in Katz v. United States, 389 U.S. 347 (1967), the critical issue whether a search or seizure has taken place came to depend upon whether one had a "reasonable expectation of privacy" — as if the underlying principle of the Fourth Amendment was to be found in future Justice Brandeis' "deep-seated abhorrence of the invasions of social privacy."[3] But the touchstone of the Fourth Amendment is not Brandeis' preoccupation with a "right to be let alone" — a respite from the hustle and bustle of daily life. Rather, the Amendment reflects Blackstone's affirmation of the duty of civil society to protect the people's active and full participation in the nation's economic life according to the "absolute right, inherent in every Englishman ... that no man's lands or goods shall be seized into the king's hands, against the great charter, and the law of

---

[3] Letter from L.D. Brandeis to S.D. Warren (Apr. 8, 1905), p. 303 in *Letters of Louis Brandeis, 1870-1907: Urban Reformer*, Vol. 1 (Urofsky & Levy eds. 1971) as cited in Dorothy J. Glancy, "The Invention of the Right to Privacy," 21 ARIZ. L. REV. 1, 6 (1979) ("The right to privacy is, as a legal concept, a fairly recent invention. It dates back to a law review article published in December of 1890 by two young Boston lawyers, Samuel Warren and Louis Brandeis.").

the land" — a right that cannot be compromised by civil government.

> So great ... is the regard of the law for private property, that it will not authorize the least violation of it; no, not even for the general good of the whole community. [1 Blackstone's Commentaries at 134-35.]

In Jones, the Supreme Court recharted its Fourth Amendment path, reasserting that the original text was plainly designed to protect private property, not privacy.[4] *See* Jones at 404-08. *See also* Florida v. Jardines, 133 S.Ct. 1409, 1414, 1417 (2013). Thus, the Court consigned the reasonable-expectation-of-privacy test to a secondary role, not the *sine qua non* as to whether there was a Fourth Amendment search. Jones at 406. In sum, the Court ruled in Jones, the privacy test functioned only as an add-on, but not a substitute for, the common law property rights of the people in their persons, houses, papers, and effects, as reflected in the private property principles, such as those stated in Blackstone's Commentaries. *See* Jardines at 1414-15.

---

[4] *See generally* H. Titus & W. Olson, "*United States v. Jones*: Reviving the Property Foundation of the Fourth Amendment," CASE WESTERN RESERVE J. OF LAW, TECHNOLOGY & THE INTERNET, vol. 3, no. 2 (Spring 2012).

B. The Sixth Circuit Elevated the Judicially Created Privacy Test Over the Fourth Amendment's Property Principles.

Although the court below acknowledged this Court's return to the Fourth Amendment's founding private property principle, it did so half-heartedly, conceding that the property principle applied only to a limited class of "government trespasses." United States v. Carpenter, 819 F.3d 880, 886 (6th Cir. 2016). However, the court claimed the Supreme Court has moved "beyond a property-based understanding of the Fourth Amendment, to protect certain expectations of privacy as well." *Id.* Consequently, the court below erroneously assumed that the only Fourth Amendment interest at stake is whether the Defendants have "asserted [a] privacy interest in information related to personal communications." *Id.* at 886. *See also id.* at 888-90. Unsurprisingly then, the court simply announced that the "defendants **of course** lack any property interest in cell-site records created and maintained by their wireless carriers." *Id.* at 888 (emphasis added). Having limited the scope of the Defendants' privacy interest to the "content" of their communications, the court below dismissed without discussion any claimed property interest that the Defendants might have in the "information that facilitate[s] ... the communication." *See id.* at 887.

The lower court's only mention of property rights is confusingly intermixed with its discussion of privacy rights. The court asserted that "defendants ... lack any **property interest**" and then — after conducting an entirely **privacy**-based analysis — concluded that

"[t]hus ... defendants have no such ... **expectation of privacy** ... in the locational information here." *Id.* at 888 (emphasis added). Having posited that the cell phone user has no property interest in the CSLI independent of any reasonable expectation of privacy in "location information," the court below would, of course, find no violation of the Fourth Amendment. *Id.* at 888.

Even the lower court's privacy reasoning, used to decide the property issue, is suspect. Relying on Smith v. Maryland, 442 U.S. 735 (1979), the Sixth Circuit claims that a cell phone user "must know" or "should know" that his CSLI is being conveyed to third persons and thus available to others. That is not the same as "'voluntarily convey[ing]'" that information under Smith. *Id.* at 888. But, more importantly, what a person "must know" or "should know" about a service provider's action is wholly irrelevant to a proper property analysis. Rather, a person's knowledge about the realities of modern society has everything to do with whether he has a "reasonable expectation of privacy." Indeed, Smith cannot be "binding precedent," having been decided at the height of this Court's experiment with privacy at a time that the Fourth Amendment's property "baseline" was being completely ignored. A privacy-based decision simply cannot resolve a post-Jones Fourth Amendment property case.

The court below decided that, because Defendants had no protected privacy interest in the information that facilitates a communication, they "could not claim that 'his "property" was invaded' by the State's

actions." *See* Carpenter at 887. This was clear error. Treating the baseline Fourth Amendment inquiry to be one of privacy, the court below violated the property baseline teaching of Jones and Jardines. According to Jones, whatever privacy interest Defendants may have in their CSLI is a fall-back, to be assessed only when, and if, the court has found no protectable property interest. *See, e.g.*, Florida v. Jardines at 1417. These principles were not followed below.

The court below would have us understand that the Jones decision is simply an application of the common law rule of trespass. Thus, the court below would shrink Jones to its bare-boned facts. *See* Carpenter at 888-89. But Jones itself refuted this idea, noting that the Fourth Amendment property principle cannot be captured by an "'18th-century tort law'" test. Jones at 411. Rather, as Justice Scalia explained:

> What we apply is an 18th-century **guarantee** against unreasonable searches, which we believe must provide at *a minimum* the degree of protection it afforded when it was adopted. [*Id.* (bold added; italics original).]

Stated another way, the trespassory test applied in Jones does not wholly encapsulate the Fourth Amendment guarantee. However, the court below, like Justice Alito's concurrence in Jones, mistakenly takes the interpretive trespassory test applied in Jones, announcing it to be the Fourth Amendment principle of Jones. But the Fourth Amendment's protection cannot be reduced to a single judicially adopted

interpretive test, such as common-law trespass, even though that test may be sufficient to resolve "easy" cases such as Jones and Jardines. *See id.*, 133 S.Ct. at 1417.

Jones did much more than simply apply a tort-based trespassory test. It restored the Fourth Amendment's property baseline to its original historic primacy, as reflected in Lord Camden's seminal opinion in Entick v. Carrington, *supra*, and in Blackstone's Commentaries. Nothing short of a textual analysis of the Amendment's property terms - "persons, houses, papers, and effects" — is sufficient. *See, e.g.*, Jones at 404 ("It is beyond dispute that a vehicle is an 'effect' as that term is used in the Amendment."). *See also* Jardines at 1414-15 ("[T]he identity of home and what Blackstone called the 'curtilage or homestall,' for the 'house protects and privileges all its branches and appurtenants.").

II. THE WARRANTLESS SEARCH VIOLATED DEFENDANTS' FOURTH AMENDMENT PROPERTY RIGHTS IN THEIR PERSONS.

The key Fourth Amendment question in this case is whether Defendants have a Fourth Amendment property right in CSLI information which they themselves generated by use of their cell phones. *See* Carpenter at 885-86. According to the court below, the "cell-site data," although generated by Defendants' movements, "took the form of business records created and maintained by the defendants' wireless carriers." *Id.* at 885-86. Thus, the lower court dismissively declared that "defendants of course lack any property

interest in [such] cell-site records." *Id.* at 888 (emphasis added). Why is this so? Have the cell phone users no recognizable interest protected by the Fourth Amendment in a record of their movements and communications? If defendants had not purchased cell phones and contracted with cell phone providers, there would have been no "cell-site records" of any type either "created" or "maintained" by the service provider, and the location of each call would not have been recorded but for the making or receiving of such calls by defendants.

According to Blackstone, one of the three absolute rights of a "person" includes the "power of loco-motion, of changing situation, or removing one's **person** to whatsoever place one's own inclination may direct; without imprisonment or restraint, unless by due course of law." 1 Blackstone at 130. Another right of personhood includes the "free use, enjoyment, and disposal of all his acquisitions, without any control or diminution, save only by the laws of the land." *Id.* at 134. Both of these rights — of movement and commerce[5] — are rights of persons as recognized by the common law and thus are protected by the Fourth Amendment which identifies one's person as foremost among the property interests of the people. Today, many would associate "persons" with only a "right of privacy." But at the time the Fourth Amendment was ratified, the word "person" had a very different

---

[5] Webster's 1828 dictionary defines "commerce" as "an interchange or mutual change of goods ... property of any kind, between ... individuals ... by purchase and sale; trade; traffick."

meaning and connotation, paralleling 17th-century property theories of John Locke:[6]

> every Man has a Property in his own Person. This no Body has any Right to but himself. The Labor of his Body and the Work of his Hands ... are properly his. [J. Locke, Second Treatise of Government, para. 27 (facsimile ed.), reprinted in J. Locke, Two Treatises of Government, pp. 287-88 (P. Laslett, ed., Cambridge Univ. Press: 2002).]

Further, Locke reasoned that "being the Master of himself, and the Proprietor of his own Person, and the Actions ... of it," a man has "in himself the great Foundation of Property...." *Id.* at para. 44. Stanford University historian and Pulitzer Prize winner Jack Rakove explains that:

> For Locke ... the concept of property encompassed not only the objects a person owned but also the ability, indeed the right to acquire them. [J. Rakove, Revolutionaries: A New History of the Invention of America at 78 (Houghton Mifflin Harcourt: 2010).]

Applying these principles here, the modern day cell phone enhances one's freedom of movement, and multiplies one's opportunities to communicate. Both movement and communication are key elements of the property in one's own person, and both are expanded

---

[6] *See, e.g.*, B. Bailyn, The Ideological Origins of the American Revolution at 26-31 (Cambridge, Mass, 1967).

by the "cellular network," wherein strategically placed transmission towers extend the ability of a person both to communicate, and also to access his "papers," wherever he happens to be. *See* Riley v. California, 134 S.Ct. 2473, 2485 (2014). In Riley, the Supreme Court observed that "modern cell phones ... are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Id.* at 2484 (emphasis added). Under the reasonable-expectation-of-privacy test, however, such "ubiquitous" use appears to be a reason to narrow Fourth Amendment protections, as the more cell phones are used, the more it can be expected that the government will use them to spy on Americans.[7]

Although it may be true that a forcible government search for CSLI generated by the Defendants may not resemble a traditional physical common law trespass on the person, such government intrusion nonetheless gobbles up the geographical information created by the cell phone user, which is created by the "labor of his body and the work of his hands" — and at his expense. *See* Locke, *supra*. Therefore, access by the government to such information, without a warrant and probable

---

[7] The effect of a privacy-based test is that people are discouraged from "cultural and economic participation." Indeed, privacy requires a person to withdraw unto himself from society and make an attempt to keep his activities secret from the world's prying eyes. A property inquiry, however, embraces a person as an active participant in society, by putting limits on the government's ability to interfere with that participation.

cause, is a search of one's person in violation of the Fourth Amendment.

III. THE WARRANTLESS SEARCH OF THE CSLI DATA VIOLATED DEFENDANTS' FOURTH AMENDMENT PROPERTY RIGHTS IN THEIR PAPERS AND EFFECTS.

As ably argued in his opening brief, Petitioner has demonstrated that the warrantless search for, and seizure of, his CSLI information violates his Fourth Amendment protected property rights in his "papers and effects." *See* Brief for Petitioner ("Pet. Br.") at 32-35. These *amici* agree. *Amici* would add to the authorities cited by Petitioner the observation of Professor John Cribbet that "[o]nly as the individual has specific, and to a limited extent exclusive, rights over a thing, does he have that liberty of action which is vitally necessary to the preservation of a free society." J. Cribbett, Principles of the Law of Property at 7 (Foundation Press, 2d edition: 1975).

The Court must now determine whether what the Sixth Circuit terms "Cell Phone Location Information" constitutes property protected under Fourth Amendment's protection of "persons, houses, papers, and effects." Although Cell Phone Location Information did not exist a few decades ago, it should be beyond question that the Fourth Amendment does not protect only tangible "papers and effects" as they existed when the Amendment was written. Indeed, Justice Scalia rejected as "bordering on the frivolous" the notion that "only those arms in existence in the 18th century are protected by the Second Amendment,"

and further pointing out that "the Fourth Amendment applies to modern forms of search [citing Kyllo v. United States, 533 U.S. 27, 35-36 (2001)]." District of Columbia v. Heller, 554 U.S. 570, 582 (2008).

The Court's determination as to papers and effects is informed by what Warren and Brandeis, more than a century ago, termed "the growth of the legal conception of property." "The Right to Privacy," *supra*. Curiously, that very Harvard Law Review article, which is the touchstone for modern discussion of privacy rights, provides extensive analysis of property law, specifically how the law had come to protect new types of property, to the point where, even in 1890, "'property' has grown to comprise every form of possession — intangible, as well as tangible." *Id.*

In the last decade, this Court has recognized the Fourth Amendment's protection of data stored on cell phones, and even more vast amounts of data accessible via those cell phones, in the context of a search incident to arrest because, as Chief Justice Roberts summarized, of "all they contain and all they may reveal [about] 'the privacies of life....'" Riley v. California, 134 S.Ct. 2473, 2494-95 (2014). And, in Jones, this Court has demonstrated that the Fourth Amendment's "close connection to property" protects against a trespass leading to the collection of location information about an individual. Jones at 405. The question now is whether one of those subsets of data about "the privacies of life" generated by the individuals, yet held in the hands of a cell phone vendor, will be protected as fully as one's "papers and effects" were at common law.

The Sixth Circuit's opinion implies that its decision would have been different if the information seized from the cell phone provider was the "content of a communication" which it said is "protected under the Fourth Amendment," rather than "information necessary to convey it" which it terms "routing information is not" protected. Carpenter at 883-84. The major case on which the Sixth Circuit relied that was outcome determinative was Smith v. Maryland, 442 U.S. 735 (1979), which was a privacy-based case that antedated the Jones resurrection of the property basis of the Fourth Amendment.[8] Moreover, the Sixth Circuit's disregard for the disclosure of location data antedated the Jones court's identification of the manifold dangers of disclosing Global Positioning System ("GPS") data which provides a "comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." Jones at 415. Indeed, in describing the dangers of somewhat more pinpoint GPS data, Justice Scalia asserted:

> because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain **abusive law enforcement practices**: "limited police resources and

---

[8] The only other Supreme Court case cited was Ex parte Jackson, 96 U.S. 727 (1878), which found no warrant was required for a government agent to read the information set out on the outside of a mailed envelope — a very different situation indeed.

> community hostility." [*Id.* at 415-16 (citations omitted) (emphasis added).]

And, lastly, Justice Scalia described the damaging effect of government surveillance and the way in which it undermines a constitutional republic:

> Awareness that the government may be watching **chills associational and expressive freedoms**. And the government's unrestrained power to assemble data that reveal private aspects of identity is **susceptible to abuse**.... [Such data] may "**alter the relationship** between citizen and government in a way that is **inimical to democratic society**." [*Id.* (emphasis added).]

Totalitarian societies do not respect the property of their people, taking what they want, from whomever they want, whenever they want.[9] In that regard, they resemble the animal world where there is neither understanding of nor respect for ownership rights — only fear of consequences. Only mankind, created in the image of God, and subject to the timeless commandments prohibiting stealing (Eighth Commandment, Exodus 20:15; *see also* Exodus 22:3; Leviticus 19:13; Mark 10:19) and coveting (Tenth Commandment, Exodus 20:17; *see also* Proverbs 30:8-9) recognize that each person has the right to own and control his own property. Particularly in

---

[9] God warned the children of Israel about the lawless acts to which they would be subjected if they chose to be ruled by a king. *See* I Samuel 8:10-22.

constitutional republics, no government, especially one of limited, enumerated powers, may seize private property, including private and personal data, without doing violence to the covenant relationship between citizen and state.[10] That covenant is described in our nation's charter, which affirms that the very purpose of government is to secure the people's God-given rights. *See* Declaration of Independence. Indeed, only with a robust right to property, not only in oneself, but in one's possessions, can one be truly free.

The Petitioner's brief clearly demonstrates defendants' exclusive right to control disposition of his cell phone location information as part of his "customer proprietary network information" under the federal Telecommunications Act. Pet. Br. at 33-34. That analysis supports two conclusions. First, it should make no difference to the resolution of this case on property principles that the location information created by Carpenter's cell phone was held by his cell

---

[10] Contrary to the nation's founding principles, the Federal Government often has demonstrated that it has no respect for the sanctity of private communications and other forms of data, asserting whatever power that it needs to assert to access them. It has demonstrated its willingness to use its regulatory powers to coerce compliance, or threaten service providers with severe sanctions, thus making those providers complicit in Fourth Amendment violations. For example, the encrypted email provider Lavabit was forced to shut down rather than violate the rights of its customers when its founder Ladar Levison refused to install government surveillance equipment on his company's network and surrender encryption keys as the Federal Government demanded. *See* L. Levison, "Secrets, lies and Snowden's email: Why I was forced to shut down Lavabit," *The Guardian* (May 20, 2014).

phone provider.[11] The relationship between Carpenter and that provider should properly be understood to be one of bailor-bailee. As Justice Scalia explained in Jones, even if "Jones was not the owner [of the Jeep Cherokee] he had at least the property rights of a bailee" which were sufficient to assert his Fourth Amendment defense. Jones at 404 n.2. Second, since a person's CSLI cannot be accessed legally by any individual person, as Petitioner clearly demonstrates (Pet. Br. at 33-34), such information cannot be informally seized simply because the seizure is at the request of a government agent. Justice Scalia explained in the sequel to United States v. Jones that "a police officer not armed with a warrant may approach a home and knock, precisely because that is 'no more than any private citizen might do.'" Florida v. Jardines, 133 S.Ct. 1409, 1416 (2013) (citations omitted).

---

[11] Justice Sotomayor's concurring opinion in Jones warned against rote application of this court's third party privacy doctrine. *See* Jones at 417-18 (Sotomayor, J. concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties [citing Smith]. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.... I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.").

IV. THE GOVERNMENT SCHEME OF BROADCAST REGULATION HAS CONDITIONED ONE'S FULL PARTICIPATION IN MODERN SOCIETY UPON FORFEITURE OF FOURTH AMENDMENT RIGHTS.

As this Court recently noted, in order to be a full participant in American society, one must possess a cellular phone: "modern cell phones ... are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." Riley at 2484. To that, Petitioner adds that "[c]ell phones are indispensable to participation in modern society often required for employment, relied on for personal safety, and increasingly becoming essential medical treatment tools." Pet. Br. at 12, 40-42.

Privacy analysis conducted by the court below treats CSLI as though it were created by cell phone providers without involvement of the customers and without involvement by government. Section II, *supra*, discusses how this data is created and paid for by the customer. This section discusses the government's role in designing the very system of cell phone use and control that it now argues justifies its ready access to every person's private papers and effects.

The federal government has created a pervasive regulatory system to control the airwaves, with cellular companies who maintain this country's wireless network serving as government gatekeepers. These companies maintain monopolistic access to

cellular radio frequencies. Writing in concurrence in CBS v. Democratic Nat'l Committee, 412 U.S. 94 (1973), Justice Douglas noted that "the airspace ... is the common heritage of all the people." *Id.* at 162. However, when it comes to cellular frequencies, that "common heritage" has been sold to the highest bidders, and now cannot be used by ordinary Americans without engaging with the cellular providers who control the bandwidth pursuant to close government supervision. *See* ABC, Inc. v. Aereo, Inc., 134 S.Ct. 2498 (2014).

The defendants in this case, like all Americans, are caught in a government-designed web, under which they may communicate over distance on no frequency other than government-approved cellular frequencies — and are prohibited in doing even that without going through a government gatekeeper wireless provider. Thus, to participate in modern society, defendants were all but required to contract with government-sanctioned vendors such as MetroPCS and T-Mobile to obtain cellular service.

Moreover, it was the federal government that initially made a push for the creation of CSLI, forcing cellular phone manufacturers to include hardware so that phones could be tracked, and forcing cellular providers to begin collecting such data upon government demand.[12]

---

[12] As Petitioner's Brief points out, even turning off a phone's "location services" "has no impact at all upon cellular service providers' ability to log and retain the phone's location." *Id.* at 42.

Thus, in order to communicate in today's modern world, defendants were forced onto government-controlled airwaves, on a government-approved cellular network, using government-mandated technology, transmitting government-required location data. And now the Sixth Circuit has claimed that, because defendants "must know" or "should know" they were being tracked, they in essence had "voluntarily conveyed" their location to the cell phone companies who — completely independently and of their own volition — decided to collect and retain that information purely for their own business purposes. Carpenter at 888. The lower court's decision is factually and legally indefensible.

A. The FCC Pervasively Regulates the Cellular Spectrum.

Over a century ago, and four months after the sinking of the Titanic, the Radio Act of 1912 was enacted to establish a commission that would designate which airwaves would be for public use and which airwaves would be reserved for the various commercial users who needed them.[13] Thereafter, the Communications Act of 1934 created the Federal Communications Commission ("FCC"), and gave it sweeping authority to "regulat[e] ... communication by wire and radio...." Pub. L. No. 73-416, Sec. 1.

---

[13] *See* M. Lasar, "How the Titanic disaster pushed Uncle Sam to 'rule the air,'" ARS Technica (Jul. 7, 2011), https://arstechnica.com/tech-policy/2011/07/did-the-titanic-disaster-let-uncle-sam-take-over-the-airwaves/.

As far back as the 1920's, the "National Radio Conferences ... divided ... the entire radio spectrum ... into numerous bands, each allocated to a particular kind of service." National Broadcasting Co. v. United States, 319 U.S. 190, 211 (1943). Since then, this Court has assumed that "the radio spectrum **simply is not large enough to accommodate everybody**," and that "[t]he facilities of radio are limited and therefore precious; they cannot be left to wasteful use without detriment to the public interest."[14] *Id.* at 213,

---

[14] This overly broad statement reflected a lack of knowledge of the radio spectrum, significant portions of which were largely unknown and still emerging in 1934. The Court's statement may have some truth when it came to the "amplitude modulation" ("AM") radio frequencies at issue in National Broadcasting Co. — which can travel hundreds of miles — but it is demonstrably false in other circumstances.

Consider, for example, the human voice, which "operates" by "transmitting" sound waves at a frequency range of about 70-400 Hz. http://goo.gl/D7YRLU. In a crowded room full of people, if everyone started talking at the same time, no one would be able to hear anything (http://goo.gl/j2sXgZ), much the same way this Court lamented of the early days of broadcast radio that, "[w]ith everybody on the air, nobody could be heard." National Broadcasting Co. at 212. Fortunately, however, the power of the human voice to "transmit" is limited to about 10 watts (http://goo.gl/EMvMWe), and thus has a finite range. In most circumstances, a person "transmitting" speech at a typical speaking level can only be heard within a limited number of feet. That is why multiple conversations can occur within the same room, even though the "broadcasters" are all using the same spectrum of frequencies.

Similarly, unlike AM radio waves, both (i) the range and (ii) the transmitting power of cellular phones are limited, which means that significant overlap in frequency use is possible even within the same town or city. *See* Section IV.B, *infra*. With more mobile phones in the world than there are people, so far there has

217 (emphasis added).

Almost three quarters of a century ago, this Court presumed that there was "'widespread fear that in the absence of governmental control the public interest might be subordinated to monopolistic domination in the broadcasting field.'" National Broadcasting Co. at 220. Some years later, the Court moved the basis for airwave regulation from monopoly to scarcity, claiming that "[i]t quickly became apparent that broadcast frequencies constituted a **scarce resource** whose use could be regulated and rationalized only by the Government."[15] Red Lion Broadcasting Co. v. FCC, 395 U.S. 367, 376 (1969) (emphasis added).

This scheme of complete government control of the entire radio spectrum assumed "that Government can control the broadcasters because their channels are in the public domain in the sense that they use the airspace that is the common heritage of all the

---

been enough room to accommodate everyone. *See* http://goo.gl/wr2qTB.

[15] Others disagreed, believing "[t]he fallacy of this argument is obvious. The number of broadcasting frequencies is limited; so is the number of concert halls; so is the amount of oil or wheat or diamonds; so is the acreage of land on the surface of the globe. 'There is no material element or value that exists in unlimited quantity. ... Contrary to the 'argument from scarcity,' if you want to make a 'limited' resource available to the whole people, make it private property and throw it on a free, open market." A. Rand, "The Property Status of Airwaves," The Objectivist Newsletter, vol. 3, no. 4, p. 1 (Apr. 1964).

people."[16] CBS v. Democratic Nat'l Committee at 162 (Douglas, J., concurring). "In managing the spectrum, FCC and NTIA[17] have largely used a 'command-and-control' approach, which dictates how each segment of the radio spectrum can be used and who can use it."[18] Today, the summary tables alone showing the FCC's allocations of the radio spectrum encompass a whopping 176 pages — hardly order from chaos.[19]

Unfortunately, much like Soviet central planners were known to wind up with too many size 15 shoes, the FCC ended up having no idea how much bandwidth to allocate to particular uses. Thus, pursuant to Congressional action in the form of the 2012 National Broadband Plan, in 2016 the FCC began

---

[16] Ayn Rand took issue with this claim as well, noting that "'public property' is a collectivist fiction, since the public as a whole can neither use nor dispose of its 'property,' that 'property' will always be taken over by some political 'elite,' by a small clique which will then rule the public — a public of literal, dispossessed proletarians." "The Property Status of Airwaves" at 3.

[17] The FCC "administers spectrum for non-Federal use," while the National Telecommunications and Information Administration "is an operating unit of the Department of Commerce, administers spectrum for Federal use." https://www.fcc.gov/engineering-technology/policy-and-rules-division/general/radio-spectrum-allocation

[18] "Spectrum Management: Better Knowledge Needed to Take Advantage of Technologies That May Improve Spectrum Efficiency," Government Accountability Office, GAO-04-666 ("GAO") (May 2004), p.5 http://www.gao.gov/new.items/d04666.pdf.

[19] *See* https://transition.fcc.gov/oet/spectrum/table/fcctable.pdf.

a "broadcast incentive auction," whereby "TV broadcasters will sell their licensed airwaves — known as spectrum — to make room for wireless service providers, with the FCC acting as the middleman to determine prices and organize the handover."[20] This "market-esque" step was made necessary by the so-called "spectrum crunch" — which reflected the FCC's failure to properly "allocate" adequate bandwidth to the wireless market in the first place.[21] *Id.* Having "[d]ecades ago ...freely g[iven] away spectrum" to uses such as broadcast TV, it was now necessary to create a "huge pay day" for TV spectrum holders who will pass portions of their bandwidth to wireless use. *Id.*

Having justified its foray into central planning of the airwaves on the theory that there would not be enough radio spectrum to go around, in reality today's shortages have been caused not by a finite radio spectrum — but by the FCC's bandwidth

---

[20] C. Lecher, "How the FCC's massive airwaves auction will change America – and your phone service," The Verge (Apr. 21, 2016), https://www.theverge.com/2016/4/21/11481454/fcc-broadcast-incentive-auction-explained.

[21] In 2004, the GAO noted that "the disadvantages of the command-and-control approach have become increasingly apparent. For example, in October 2001, the FCC Chairman noted that it is becoming difficult for government officials to determine the best use for spectrum and to repeatedly adjust allocations and assignments of spectrum to accommodate new spectrum needs and new services. The President has similarly noted that the existing legal and policy framework for spectrum management has not kept pace with the dramatic changes in technology and spectrum use and can discourage the introduction of new technologies." GAO at 7.

mismanagement.[22] And, as with most government failures, additional intervention is always needed to solve past shortcomings, perpetuating a vicious cycle. And, as is also typical, in the case of wireless bandwidth, the American public will bear the brunt of the government's failure,[23] while the federal government stands to reap billions of dollars from its own decisions.[24]

B. Contrary to the Government Claim, the Cellular Network Is "Large Enough to Accommodate Everybody."

As Petitioner explains, "[i]n order to access the cellular network, cell phones must connect to nearby cell towers (known as 'cell sites.')." Pet. Brief at 3. In truth, cellular phones are handheld radios, albeit with

---

[22] D. Goldman, "Sorry, America: Your wireless airwaves are full," CNN Money (Feb. 21, 2012), http://money.cnn.com/2012/02/21/technology/spectrum_crunch/index.htm (noting the large increase in demand for cellular traffic, but also that "[a]nother catalyst is the way the U.S. government allocated spectrum.").

[23] "For the situation to improve, carriers — and, therefore, their customers — will have to pay more." Goldman at 2.

[24] "Of the nearly $20 billion raised [from the FCC's bandwidth auction], **more than $6 billion will go to reduce the U.S. deficit**, more than $10 billion will go to broadcasters that chose to relinquish spectrum rights, and up to $1.75 billion for other broadcasters that incur costs in changing channels." (emphasis added). D. Shepardson, "FCC spectrum auction bidding ends at $19.6 billion," Reuters (Feb. 10, 2017), http://www.reuters.com/article/us-usa-wireless-auction-idUSKBN15P2QF.

staggering capabilities.[25] Indeed, all of the information transmitted to and from a cellular phone — phone calls, text messages, internet browsing, video, pictures, apps, etc. -- is transmitted via radio waves. And all of this occurs over frequencies that have been designated by the FCC for commercial use by wireless providers.

As part of the FCC's modern allocation of the radio spectrum, it has decided on which bandwidth cellular communications may take place: "[t]he FCC also decides which frequencies of spectrum can be used for which purposes. For mobile phones, it has allocated spectrum generally between 700 MHz and 2.6 GHz."[26] Currently, cellular and wireless communications take place largely on the "824 – 849 and 869 – 894 MHz spectrum range" (the "Cellular" band) and "the 1850 – 1990 MHz spectrum range" (the "Broadband Personal Communications Service" band), with other smaller allocations in the "Advanced Wireless Service" band, the 700MHz band, etc.[27] All of these bands are within what is known as the "ultra-high frequency" ("UHF") spectrum, which is classified as frequencies between 300 MHz and 3GHz.[28]

---

[25] *See* https://www.mat.ucsb.edu/~g.legrady/academic/courses/03w200a/projects/wireless/cell_technology.htm.

[26] *See* https://www.cnet.com/news/wireless-spectrum-what-it-is-and-why-you-should-care/.

[27] *See* https://www.fcc.gov/wireless/bureau-divisions/mobility-division/cellular-service.

[28] *See* http://www.arrl.org/files/file/Get%20Licensed/HRLM%201st/Corrections/2-17_rev.pdf.

Generally, UHF radio waves "travel almost entirely by line-of-sight propagation ... and ground reflection; unlike High Frequency ("HF") and Very High Frequency ("VHF"), there is little to no reflection from the ionosphere (skywave propagation), or ground wave."[29] Due to this line-of-sight characteristic, "**UHF transmission is limited** by the visual horizon to 30 -40 miles ... and often to shorter distances by local terrain...." *Id.* In addition to the low range of cellular frequencies, cellular phones transmit with **relatively low power** — a few watts or less.[30] Even cellular towers (which retransmit signals) use comparatively low power transmitters. *Id.*

In sum, the UHF radio waves on which cellular technology operates allows for large amounts of data to be transmitted and received quickly, while the low range allows for significant "reuse" of frequencies — even across the same city — by multiple cell phones. However, what is a strength of the UHF band is also a weakness — since the range of UHF radio waves is inherently limited, this created the need for cellular towers and providers to retransmit signals over longer distances (across states, the country, and the world). In other words, the FCC regulatory scheme has made it necessary for public mobile communications to

---

[29] *See* https://en.wikipedia.org/wiki/Ultra_high_frequency#Propagation_characteristics; *see also* The ARRL Ham Radio License Manual, American Radio Relay League, 3rd edition (May 15, 2014).

[30] *See* https://www.mat.ucsb.edu/~g.legrady/academic/courses/03w200a/projects/wireless/cell_technology.htm.

utilize the current cellular network through wireless providers.

C. The FCC Has Made Cellular Providers Necessary and Helps Them Protect Their Turf from Competing Technologies.

Because cellular phones are radio transmitters and receivers, they are capable of communicating directly with one another at short range — such as across town — without involvement of the cellular network. In fact, in recent years Qualcomm has been experimenting with a system called "LTE Direct," whereby phones will act as two-way radios, and "will be able to 'talk' directly to other mobile devices and to beacons," so long as they are within a range of 500 meters.[31] Similarly, researchers in Australia have developed a system where a grid of interconnected cellular phones will be able to act as its own cellular network by receiving and re-transmitting signals sent by other phones in the network.[32]

At first blush, these new technologies sound like they soon could increase the freedom of a phone user by negating the need for cellular providers, but that is not the case. Unfortunately, because of the FCC and the federal government's monopoly of the radio

---

[31] *See* https://www.technologyreview.com/s/530996/future-smartphones-wont-need-cell-towers-to-connect/.

[32] *See* D. Quick, "No mobile phone coverage? No worries, researchers put a tower in a phone," New Atlas (Jul 12, 2010), http://newatlas.com/serval-mobile-phone-network/15696/.

spectrum, "carriers will [still] control ... devices on their networks ... because [they] use[] the same radio spectrum as conventional cellular links" — spectrum over which the FCC has given the providers total control.[33]

The need for cellular providers also could be lessened is through the use of signal boosters. "Signal boosters are devices that hold great potential to improve wireless coverage to areas with poor signal levels."[34] Purchased and installed by any third party, signal boosters are essentially "mini cellular towers" that extend the range of a cell phone tower to locations with poor reception.[35]

However, as with direct phone-to-phone communication, it did not take long before "[c]arriers complained that these devices were operating in their exclusive space and disrupting their service."[36] In

---

[33] T. Simonite, "Future Smartphones Won't Need Cell Towers to Connect," MIT Technology Review (Sep. 29, 2014), https://www.technologyreview.com/s/530996/future-smartphones-wont-need-cell-towers-to-connect/.

[34] *See* https://www.fcc.gov/rulemaking/10-4.

[35] *See* E. Falcon, "FCC Helped Create the Stingray Problem, Now it Needs to Fix It," Electronic Frontier Foundation ("EFF") (Oct. 6, 2016), https://www.eff.org/deeplinks/2016/08/fcc-created-stingray- problem-now-it-needs-fix-it?page=2.

[36] *See* EFF at 3.

2013, the FCC issued a 106-page Report and Order,[37] cracking down on the use of signal boosters, severely limiting their use, and requiring their registration with the provider on whose network they operate. *Id.* at 35. Although still permissible in some forms, the FCC's Order ensured that most wireless communications will continue to be transmitted through towers owned by cellular providers, where they can be most easily tracked.[38]

D. CSLI Is Not "Voluntarily Conveyed" to Wireless Providers, But Is Mandated by Government.

Nearly 20 years ago, in an article entitled "'E911' Turns Cell Phones Into Tracking Devices," *Wired Magazine* informed tech-savvy members of the public of a recent action by Congress.[39] As part of the Wireless Communications and Public Safety Act of 1999 ("9-1-1 Act"), Congress amended 47 U.S.C. § 222, "privacy of customer information," adding an exception for wireless carriers "to provide call location

---

[37] *See* https://apps.fcc.gov/edocs_public/attachmatch/FCC-13-21A1.pdf.

[38] Meanwhile, though, the FCC has permitted the wide use by state and local governments and police agencies of "stingrays," or "cell site simulators," which trick cellular phones in a given area to connect to the false "tower" and transmit their location information to the government's prying eyes. *See* EFF at 1.

[39] C. Oakes, "'E911' Turns Cell Phones into Tracking Devices," Wired Magazine (Jan. 6 , 1998), https://www.wired.com/1998/01/e911-turns-cell-phones- into-tracking-devices/.

information concerning the user of a commercial mobile service ... in order to respond to the user's call for emergency services...."[40] Subsequent to the 9-1-1 Act, the FCC took the additional step of "requir[ing] wireless telephone carriers to provide 911 and E911 capability, where a Public Safety Answering Point (PSAP) requests it [to] provide an accurate location for 911 calls from wireless phones."[41] Phase I of the FCC's requirements forced wireless providers to provide "the location of the cell site or base station transmitting the call," while Phase II required even more precise location information be reported. *Id.*

As reported by *Wired*, as far back as 1998 the FCC's rules "ha[d] others calling for restrictions on how cell-locating information can be used." *Id.* It was reported that "[t]o provide this precise location information ... the Cellular Telecommunications Industry Association says different carriers will choose different methods of gathering location information, but all of them involve detecting the radio frequencies sent from the phone to service antennas." *Id.* Privacy advocates in vain called for "clear restrictions on the ability of law enforcement to tap into personal information on users, especially their whereabouts at any one time." *Id.*

---

[40] *See* Pub. L. 106–81, Wireless Communications and Public Safety Act of 1999 (Oct. 26, 1999), https://www.congress.gov/106/plaws/publ81/PLAW-106publ81.pdf.

[41] "911 and E911 Services", FCC, Jul. 31, 2017, https://www.fcc.gov/general/9-1-1-and-e9-1-1-services.

E. CSLI Records Are Required by the Government.

In this case, the Sixth Circuit concluded that MetroPCS and T-Mobile "made records, for billing and other business purposes." Carpenter at 886. That may be partially true, but more importantly than business purposes, wireless providers gather CSLI because federal law requires them to do so. The Sixth Circuit wholly ignores the significance of those federal mandates.

Instead, analogizing this case to Smith, where this Court held that the user of a land line telephone "voluntarily conveyed" to the phone company the number he was dialing, the court below asserted that the defendants in this case "must know" and "should know" that their phones "'expose[]' [their] location to the nearest cell tower and thus to the company that operates the tower." Carpenter at 888. Of course, the lower court could not directly claim that defendants here "voluntarily conveyed" their CSLI to their providers[42] — because, as the lower court is quick to claim, CSLI is "gathered" by the phone companies rather than "conveyed" by phone users. In likening this case to Smith, the Sixth Circuit has taken a case where someone knowingly took a voluntary action himself, and analogized it to a situation where that person "should know" that a third party is taking an

---

[42] At the petition stage, the government, however, had no problem claiming making this assertion. *See* Brief for the United States in Opposition at 8.

action (at government direction) over which he has no control.

It was Congress and the FCC that pushed for the creation and collection of CSLI. The Sixth Circuit discussed only the current business purposes of wireless providers — without addressing the broader picture — giving an inaccurate concept of CSLI, what it is, why it is collected, and to whom it belongs. It would be unconscionable for a court to hold that a person has no Fourth Amendment right to keep the government from tracking his cell phone, when it is, in some part, federal law and regulation that requires the cell phone to be tracked. Legalization of constitutional violations does not make them constitutional.

F. Summary.

It is the federal government that has mandated cellular communication only take place on certain bands of frequencies — and that has prohibited similar communications on all other frequencies.[43] And it is

---

[43] To be sure, there are certain narrow bands of frequencies that have been set aside for amateur radio use ("ham radio"). However in order to communicate on those frequencies, a person first must pass an FCC test, and his transmissions must comply with a host of stringent FCC regulations. For example, §97.113 of the FCC's rules governing amateur radio state that "No amateur station shall transmit ... messages encoded for the purpose of obscuring their meaning ..." The same FCC rule also governs what can be said, prohibiting the transmission of music, messages for material compensation or pecuniary gain, and any form of "broadcasting." And, most importantly, the FCC bans "Communications, on a regular basis, which could reasonably be furnished alternatively

the government that has selectively doled out those frequencies to its chosen gatekeepers, the wireless carriers, mandating that no one else (especially not private persons) may use the frequencies on their own. The government then has protected the "turf" of those wireless carriers, insulating them from competing and emerging technologies that have the potential to turn wireless providers into dinosaurs, and make the cellular network obsolete and unnecessary.

So as not to exist as hermits, self-ostracized from American society, defendants chose to obtain cellular phones and, having done so, were required to contract with one of the government's approved carriers. It was the government that then forced them to run their communications through these carriers, transmit to the carriers' towers, and divulge their location information. All this, the Sixth Circuit claims, was entirely voluntary and justified, ignoring the fact that the government designed the system which now allows it to engage in Orwellian surveillance of the American public, tracking every person with a cell phone virtually every minute of his life.

CONCLUSION

For the foregoing reasons, this Court should determine that warrantless search and seizure of CSLI violates the Fourth Amendment and reverse the judgment of the court below, as well as remand

---

through other radio services" — presumably such as cellular phone calls.

Graham v. United States, No. 16-6308, to the Fourth Circuit, ordering that the decision below be vacated.

Respectfully submitted,

JOSEPH W. MILLER
U.S. Justice Foundation
932 D Street, Ste. 2
Ramona, CA 92065-2355
Attorney for Amicus Curiae
U.S. Justice Foundation

MICHAEL BOOS
Citizens United
1006 Pennsylvania Ave, SE
Washington, D.C. 20003
Attorney for Amici Curiae
Citizens United and
Citizens United Foundation

J. MARK BREWER
BREWER & PRITCHARD
Three Riverway, 18th Floor
Houston, TX 77056
Attorney for Amicus Curiae
Conservative Legal Defense
and Education Foundation

ROBERT J. OLSON*
HERBERT W. TITUS
WILLIAM J. OLSON
JEREMIAH L. MORGAN
WILLIAM J. OLSON, P.C.
370 Maple Ave. W., Ste. 4
Vienna, VA 22180-5615
(703) 356-5070
wjo@mindspring.com
Attorneys for Amici Curiae

**Counsel of Record*
August 14, 2017

RECORDS AND BRIEFS

FILED
SEP 29 2017
OFFICE OF THE CLERK
SUPREME COURT, U.S.

No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,
PETITIONER,

v.

UNITED STATES OF AMERICA,
RESPONDENT.

On Writ of Certiorari to the
United States Court of Appeals for the Sixth Circuit

BRIEF OF *AMICUS CURIAE* MICHAEL VARCO IN SUPPORT OF RESPONDENT

Michael Varco
Counsel of Record and
Amicus Curiae
P.O. Box 2548
Reston, VA 20195
(703) 635-7903
m_varco@yahoo.com

September 29, 2017

QUESTION PRESENTED

Whether the government's acquisition, pursuant to a court order, of historical mobile-device location records maintained by a third party violates the Fourth Amendment rights of the individual owner of the mobile device to whom the records pertain.

TABLE OF CONTENTS

Page

QUESTION PRESENTED i

TABLE OF AUTHORITIES iii

INTEREST OF AMICUS CURIAE 1

BACKGROUND 3

SUMMARY OF ARGUMENT 4

ARGUMENT 7

I. The Digital Age Does Not Necessitate Changes to the Third-Party Doctrine. 7

A. Justice Sotomayor's Suggestion in *Jones* to Reconsider the Third-Party Doctrine Overlooks What the Government Learns from Other Sources and How Crime Harms Victims. 8

B. Cell Phone Users Have More Control Over Providing CSLI to Service Providers Than Crime Victims May Have Over Revealing Sensitive Information About Themselves. 13

C. The Third-Party Doctrine Is More Important Than Ever in the Digital Age Because of "Substitution Effects" 14

D. Laws Are the Best Way to Address Privacy Issues with the Third-Party Doctrine. 18

E. Markets Also Respond to Privacy Concerns from the Public. 19

II. The Past Use of Tracking Dogs to Determine Historical Location Information Is Analogous to Acquiring Historical CSLI. 20

III. People Lack a Reasonable Expectation of Privacy in Historical CSLI. 22

A. Before December 2010, Many Sources (e.g., FCC Rules, News, Manuals, Patents, and Movies) Informed the Public that Cell Phones Provided CSLI to Third Parties. 23

B. Today, People Have More Reasons to Know Their Cell Phones Provide CSLI to Third Parties. 25

Conclusion 26

TABLE OF AUTHORITIES

Page(s)

CASES

Citizens United v. Federal Election Com'n, 130 S.Ct. 876 (2010) 13

City of Los Angeles v. Patel, 135 S.Ct. 2443 (2015) 11

Communist Party of the United States v. SACB, 367 U.S. 1 (1961) 13

Page(s)

Florida v. Jardines,
133 S.Ct. 1409 (2013) 21, 22

Illinois v. Caballes,
125 S.Ct. 834 (2005) 21

Katz v. United States,
389 U.S. 347 (1967) 5

Kyllo v. United States,
533 U.S. 27 (2001). 22

New York ex rel. Bryant v. Zimmerman,
278 U.S. 63 (1928) 12

Smith v. Maryland,
442 U.S. 735 (1979) 7

United States v. Carpenter,
819 F.3d 880 (6th Cir. 2016) 3, 4, 5, 22

United States v. Diaz-Castaneda,
494 F.3d 1146 (9th Cir. 2007) 17

United States v. Jacobsen,
104 S.Ct. 1652 (1984) 21

United States v. Jones,
132 S.Ct. 945 (2012) 7, 8, 10, 11, 18, 22

United States v. Miller,
425 U.S. 435 (1976). 15

United States v. Place,
103 S.Ct. 2637 (1983) 21

United States v. Walraven,
892 F.2d 972 (10th Cir. 1989). 17

Page(s)

STATUTES

18 U.S.C. § 2703(d) 6, 11, 18, 19

CONSTITUTIONAL PROVISIONS

U.S. Const. amend. I..... 4, 11, 16, 17

U.S. Const. amend. IV .....passim

REGULATIONS

47 C.F.R. § 20.18..... 23, 24

OTHER AUTHORITIES

Accenture, *Banking Technology Vision 2017*, https://www.accenture.com/t20170322T205838Z__w__/us-en/_acnmedia/PDF-47/Accenture-Banking-Technology-Vision-2017.pdf#zoom=50. 16

ACLU, *Cell Phone Location Tracking Laws By State*, https://www.aclu.org/issues/privacy-technology/location-tracking/cell-phone-location-tracking-laws-state?redirect=map/cell-phone-location-tracking-laws-state..... 18

Apple, *Find My iPhone*, https://www.apple.com/icloud/find-my-iphone. 25

Apple, *iPhone User Guide* (2009), https://manuals.info.apple.com/MANUALS/0/MA616/en_US/iPhone_iOS3.1_User_Guide.pdf..... 7, 24

Page(s)

Ariel Barkhurst, *Robbers turn to rental cars to avoid detection*, AZ Sentinel, Apr. 12, 2012, http://articles.sun-sentinel.com/2012-04-03/news/fl-rental-cars-used-in-robberies-20120402_1_rental-cars-rental-vehicles-surveillance-cameras. 17

AT&T, *AT&T Transparency Report*, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html. 8

Blake E. Reid, Comment, *Substitution Effects: A Problematic Justification for the Third-Party Doctrine of the Fourth Amendment*, 8 J. ON TELECOMM. & HIGH TECH. L. 613 (2010) 14

Ctr. for Medicare and Medicaid Serv., OMB No. 0938-0008, https://www.cms.gov/Medicare/CMS-Forms/CMS-Forms/downloads/cms1490s-english.pdf. 9

Devin Dwyer et al., *Rape Kit Testing Backlog Thwarts Justice for Victims*, ABC News, May 20, 2010, http://abcnews.go.com/Politics/sexual-assault-victims-congress-solve-rape-kit-backlog/story?id=10701295. 10

FBI, *Crime in the United States 2015*, https://ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015/tables/table-1 12

Page(s)

FCC, *FCC Report to Congress on the Deployment of E-911 Phase II Services By Tier III Service Providers* (Mar. 23, 2005), https://apps.fcc.gov/edocs_public/attachmatch/DOC-257626A1.pdf 23

James Barron, *How a Son of Sam Detective Realized 'This Has Got to Be the Guy'*, N.Y. Times, Aug. 6, 2017, https://www.nytimes.com/2017/08/06/nyregion/son-of-sam-killings-david-berkowitz.html. 16

Kim C. Thornton, Bloodhounds (1998) 5, 21

Libelium, *Meshlium Xtreme Technical Guide*, (v. 7.3, July 2017), http://www.libelium.com/downloads/documentation/meshlium_technical_guide.pdf 20

M. Licea, *Serial killer with shipping container dungeon: My victims had it coming*, N.Y. Post, Sept. 9, 2017, http://nypost.com/2017/09/09/serial-killer-says-he-was-trying-to-save-woman-he-kept-in-shipping-container 19

Mark Bergen, *Google Will Stop Reading Your Emails for Gmail Ads*, Bloomberg Tech., June 23, 2017, https://www.bloomberg.com/news/articles/2017-06-23/google-will-stop-reading-your-emails-for-gmail-ads. 19

NACVB, *Crime Victim Compensation: An Overview*, http://www.nacvcb.org/index.asp?bid=14. 9

Page(s)

Nat'l Archives, *From Benjamin Franklin to Richard Jackson, 25 June 1764*, https://founders.archives.gov/documents/Franklin/01-11-02-0064 21

Nate Anderson, *How "cell tower dumps" caught the High Country Bandits – and why it matters*, ARS Technica, Aug. 29, 2013, https://arstechnica.com/tech-policy/2013/08/how-cell-tower-dumps-caught-the-high-country-bandits-and-why-it-matters. 20

Orin Kerr, *Symposium: Carpenter and the Eyewitness Rule*, SCOTUSblog, (Aug. 4, 2017, 1:39 PM), http://www.scotusblog.com/2017/08/symposium-carpenter-eyewitness-rule. 11

Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) 14

RAINN, *What is a Rape Kit?*, https://www.rainn.org/articles/rape-kit. 10

Ryan Hutchins, *Cell phone tracking software helps police, emergency workers*, NJ.com, Jun. 22, 2009, http://www.nj.com/news/index.ssf/2009/06/cell_phone_tracking_software_h.html. 25

Sup. Ct. D.C., *Crime Victims Compensation Program Brochure*, http://www.dccourts.gov/internet/documents/CVCP_Brochure.pdf. 9

Suspect in Kelsey Smith's Death Charged with Murder, Kidnapping, FoxNews.com, June 7, 2007, http://www.foxnews.com/story/2007/06/07/suspect-in-kelsey-smith-death-charged-with-murder-kidnapping.html 24

Tara C. Jatlaoui et al., *Abortion Surveillance - United States, 2013*, MMWR, Nov. 25, 2016, http://dx.doi.org/10.15585/mmwr.ss6512a1 9

The Recruit (Touchstone Pictures 2003) 25

U.S. Census Bureau, *Health Insurance Coverage in the US: 2015*, 1, https://www.census.gov/content/dam/Census/library/publications/2016/demo/p60-257.pdf 9

U.S. Patent No. 5,519,760 (filed June 22, 1994) 24

U.S. Patent No. 7,515,578 abs. (filed May 8, 2006) . 24

U.S. Patent No. 8,073,460 (filed Mar. 29, 2007) 24

Uber not the only ride-hailing company with sights set on driverless cars, AP, Sept. 18, 2016, https://www.cbsnews.com/news/uber-not-the-only-ride-hailing-company-with-sights-set-on-driverless-cars-lyft/. 17

Uber, *Ride*, https://www.uber.com/ride 25

Verizon, *United States Report*, http://www.verizon.com/about/portal/transparency-report/us-report. 8

Wash. Univ. in St. Louis, *Rape Trauma Syndrome*, https://rsvpcenter.wustl.edu/learn-more/rape-trauma-syndrome. 12

YouTube, *The Heist: Make Experience Your Business | Adobe Experience Cloud*, https://www.youtube.com/watch?v=_KOuliSqSJo..... 14

INTEREST OF AMICUS CURIAE[1]

As a crime victim, I have a personal obligation to share my concerns with this Court. While the constitutional rights of the accused matter, I do not want to see the interpretation of the Fourth Amendment change in a way that could hinder criminal investigations.

Also, I want this Court to understand how frustrating it has been to observe all the ways that companies track the locations of mobile devices – when users let them do so – only to see none of that information available to help me. Sharing my experience may help other crime victims too.

On July 31, 2016, I was a victim of an unprovoked assault in the Dupont Circle area of Washington DC. I suffered many fractures to my face and my jaw. The first two facial-trauma surgeons that I consulted could not perform the first surgery I needed. I cannot identify those involved with the assault; however, I hope that the detective assigned to my case may find more leads using cell-phone location information (CPLI). Herein, CPLI refers to location information based on one or more technologies (e.g., GPS, CSLI, Wi-Fi, etc.).

---

[1] Both parties have consented to all amicus briefs. No counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than amicus curiae made a monetary contribution to its preparation or submission.

After the assault, I asked the detective to pursue relevant CPLI. I showed the detective a Google Timeline[2] from when the attack occurred. The Google Timeline showed a map of my phone's historical location, possibly from cellular and Wi-Fi signals my phone provided. The Google Timeline placed me at a 7-Eleven, steps from the assault. It indicated when I walked and when I took a vehicle. It placed me at the hospital later. When a nurse took a photo of me with my phone, Google put the photo on the Google Timeline. Because Google traced CPLI related to me, I thought Google – or another company – may have traced CPLI related to those near me during the crime. I thought relevant CPLI could identify people in the detective's video evidence.[3]

The detective requested the CPLI of those near me, but the prosecutor with decision-making authority declined the CPLI request. Fourth Amendment concerns may have been a factor in denying the CPLI request. For this reason, I hope that this Court will soon explain what limits, if any, an individual's Fourth Amendment rights put on the government acquiring CPLI from a third party to support a criminal investigation.

---

[2] For information about Google Timeline, see Google, *Google Maps Help*, https://support.google.com/maps/answer/6258979?co=GENIE.Platform%3DDesktop&hl=en.

[3] YouTube, *Persons of Interest in Aggravated Assault*. 1100 b/o 19th St. NW, on July 31, 2016, https://www.youtube.com/watch?v=MdrjECC1r1E&feature=youtu.be (uploaded May 16, 2017).

If this Court affirms the Sixth Circuit, then I hope that the government will use CPLI more effectively in criminal investigations, when appropriate. The government's capabilities for using CPLI in criminal investigations should catch up with other areas of forensics.

BACKGROUND

A jury convicted Timothy Ivory Carpenter and Timothy Michael Sanders of charges related to robberies in the Detroit area from December 2010 to April 2011. Based on cell phone numbers that one of their co-conspirators gave the FBI, the FBI applied for orders from magistrate judges to obtain cell-site location information (CSLI) from various wireless carriers without a warrant. The magistrate judges granted the FBI's requests for CSLI. The CSLI showed that Sander's and Carpenter's phones were within a half-mile to two miles of the location of each of the robberies around the time of the robberies.

The government used the CSLI at trial. Carpenter and Sanders appealed their convictions on the grounds that the government acquired the CSLI in violation of their Fourth Amendment rights. The Sixth Circuit affirmed both convictions, deciding that the government's acquisition of CSLI was not a search.[4]

---

[4] *United States v. Carpenter*, 819 F.3d 880, 884-86, and 890 (6th Cir. 2016).

SUMMARY OF ARGUMENT

Some would like this Court to believe that, due to new technologies in the digital age, an Orwellian state with constant surveillance is imminent.

This case does not justify those fears. In the present case, the government acquired historical cell-site location information (CSLI) to support a criminal investigation, not to track the public at large. In free societies, people expect their governments to investigate and prosecute criminal activity.

There are at least three reasons why this Court should decide the Fourth Amendment allows the government to acquire historical CSLI from a third party, pursuant to a court order.

First, the third-party doctrine should apply to CSLI. Under the third-party doctrine, a person lacks a reasonable expectation of privacy – and therefore lacks Fourth Amendment protection – in information voluntarily provided to a third party.[5] The third-party doctrine makes sense because a person's Fourth Amendment rights should not stop third parties from exercising their First Amendment rights and disclosing what they know to the government. Because cell phone users voluntarily provide CSLI to their service providers (i.e., third parties), cell phone users should not have Fourth Amendment protection in CSLI and/or other CPLI.

---

[5] *See id.* at 889.

Second, obtaining historic location information using dogs is analogous to CSLI; thus, dogs may be just as relevant as *Katz*.[6] CSLI could be considered a phone's digital scent trail, similar to a person's physical scent trail. Governments have used dogs for centuries to determine historic location information by tracking the physical scents of people. In fact, Benjamin Franklin tried to acquire bloodhounds in order to locate people accused of crimes.[7] Benjamin Franklin's past actions are relevant to colonial-era views about acquiring historical location information in criminal investigations. If the government does not need a warrant to determine a person's historical location by using a dog, then this Court should not require a warrant to determine the historical location of a device by acquiring CSLI.

Third, in addition to the reasons provided by the Sixth Circuit,[8] many other sources (e.g., news coverage, device manuals, movies, patents, FCC rules, etc.) show that people lack a reasonable expectation of privacy in historical CSLI.

---

[6] Part of the Sixth Circuit's opinion discusses *Katz* because CSLI does not belong to one of the protected elements in the text of the Fourth Amendment (e.g., persons, houses, papers, and effects). U.S. Const. amend. IV; *Carpenter*, 819 F.3d at 886 (deciding that the government's acquisition of CSLI was not a search, based on the two-part test in *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J. concurring)).

[7] Kim C. Thornton, *infra*, note 44 at 10.

[8] *Carpenter*, 819 F. 3d at 888 (discussing cell-signal strength indicators and roaming charges as CSLI indicators).

When deciding whether to apply the third-party doctrine to CSLI, this Court should consider the privacy and freedom interests of crime victims alongside those of crime suspects. Crime victims lose substantial privacy when they apply for crime victim's compensation, undergo rape kit exams, etc. Crime victims may have disfiguring injuries that reveal sensitive information to others. Results of crime, such as trauma and death, unjustly harm the associational and expressive freedoms of crime victims far more than CSLI could possibly harm crime suspects. Accordingly, in order to help law enforcement prosecute violent criminals and to prevent future crime victims, this Court should apply the third-party doctrine to CSLI.

Additionally, new technologies make the third-party doctrine more important than ever in the digital age. For example, artificial intelligence may replace human witnesses; consequently, law enforcement may have to rely on the third-party doctrine to obtain information that witnesses previously would have provided.

People that disagree with the current law can lobby Congress and/or state representatives to change the law. Alternatively, people can move to states that add a warrant requirement to 18 U.S.C. § 2703(d). This Court does not have to intervene.

Accordingly, the judgement of the Sixth Circuit Court of Appeals should be affirmed.

ARGUMENT

I. The Digital Age Does Not Necessitate Changes to the Third-Party Doctrine.

In modern times, third parties may use various technologies (e.g., CSLI, GPS, Wi-Fi) to determine the approximate locations of mobile devices (e.g., cell phones). The technologies determine the locations of mobile devices based on information the mobile devices provide to cell towers, GPS satellites, Wi-Fi access points, etc.[9]

Under the third-party doctrine, people have "no legitimate expectation of privacy" in information voluntarily given to third parties[10]; therefore, under prior precedents, a person's Fourth Amendment rights may not protect him from the government's acquisition of CPLI from third parties.

However, Justice Sotomayor has suggested revisiting the third-party doctrine in the digital age because of concerns that the government might use location monitoring to obtain extensive and intimate details about people.[11]

---

[9] *See* Apple, *iPhone User Guide*, p. 144 (2009), https://manuals.info.apple.com/MANUALS/0/MA616/en_US/iPhone_iOS3.1_User_Guide.pdf (describing Location Services).

[10] *Smith v. Maryland*, 442 U.S. 735 (1979).

[11] *United States v. Jones*, 132 S.Ct. 945, 955 (2012) (Sotomayor J., concurring) (citation omitted) ("Disclosed in [GPS] data . . . will be . . . trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel . . . .").

A. Justice Sotomayor's Suggestion in *Jones* to Reconsider the Third-Party Doctrine Overlooks What the Government Learns from Other Sources and How Crime Harms Victims.

The privacy issues that Justice Sotomayor discusses in *Jones* are minor compared to what the government learns from other sources and how crime impacts the privacy and freedoms of crime victims.

1. Medical Information

First, in *Jones*, Justice Sotomayor suggests that the government might infer people's medical information from location monitoring in criminal investigations.[12] Her concern overlooks how the government learns far more from its healthcare role and/or from crime victims than it could possibly infer from CSLI pertaining to crime suspects.

Many companies report how many location requests they receive. From July 2016 to June 2017, AT&T received 52,139 requests for historic CSLI.[13] In the first half of 2017, Verizon received 20,442 requests for location information, but a quarter had warrants.[14] It is unclear if any of the requests let the government infer medical information.

---

[12] *Id.*

[13] AT&T, *AT&T Transparency Report*, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html.

[14] Verizon, *United States Report*, http://www.verizon.com/about/portal/transparency-report/us-report.

By comparison, the government learns far more from its healthcare role than it could possibly infer from historical CSLI. The US government covers health insurance for over 118 million people.[15] When the government pays a medical claim, the government learns someone's medical information (e.g., code for illness and test).[16] Also, since 1969 the CDC has kept detailed abortion statistics (e.g., mother's age, race, gestation, etc.).[17]

Also, crime victims reveal far more sensitive information to the government than the government could infer from CSLI. To apply for crime victim's compensation, crime victims may need to provide the government copies of their medical bills, lost wages, and mental-health bills.[18] The US pays "close to $500 million yearly to more than 200,000 victims" through crime victim compensation programs.[19]

---

[15] U.S. Census Bureau, *Health Insurance Coverage in the US: 2015*, tbl. 1, https://www.census.gov/content/dam/Census/library/publications/2016/demo/p60-257.pdf (2015 statistics).

[16] See e.g., Ctr. for Medicare and Medicaid Serv., *OMB No. 0938-0008*, https://www.cms.gov/Medicare/CMS-Forms/CMS-Forms/downloads/cms1490s-english.pdf.

[17] Tara C. Jatlaoui et al., *Abortion Surveillance - United States, 2013*, MMWR, Nov. 25, 2016, http://dx.doi.org/10.15585/mmwr.ss6512a1 (prepared by CDC).

[18] Sup. Ct. D.C., Crime Victims Compensation Program Brochure p. 3, http://www.dccourts.gov/internet/documents/CVCP_Brochure.pdf.

[19] NACVB, *Crime Victim Compensation: An Overview*, http://www.nacvcb.org/index.asp?bid=14.

Also, medical personnel perform about 180,000 sexual assault forensic exams yearly.[20] In those exams, crime victims may have to endure a full physical examination and/or may have to share their medical and sexual history – shortly after trauma.[21]

Because violent criminals may harm again, preserving the third-party doctrine may reduce how much private medical information the government learns about people; therefore, applying the third-party doctrine to CSLI is important. With the right tools, law enforcement may get the evidence it needs to convict more violent criminals; fewer violent criminals may harm fewer crime victims; and fewer crime victims may suffer impacts to their privacy.

2. Associational and Expressive Freedom

Second, in *Jones,* Justice Sotomayor expresses concern that the government might have unfettered discretion to track anyone; thus, "Awareness that the Government may be watching chills associational and expressive freedoms."[22] However, in the present case, the government's acquisition of historical CSLI pursuant to a court order poses little risk of moving this nation towards an Orwellian State.

---

[20] *See* Devin Dwyer et al., *Rape Kit Testing Backlog Thwarts Justice for Victims*, ABC News, May 20, 2010, http://abcnews.go.com/Politics/sexual-assault-victims-congress-solve-rape-kit-backlog/story?id=10701295.

[21] RAINN, *What is a Rape Kit?*, https://www.rainn.org/articles/rape-kit.

[22] *Jones,* 132 S.Ct. at 956 (citation omitted).

For starters, the government lacks unfettered discretion to track and/or acquire anyone's location information. Third parties may oppose government efforts to acquire the location information.[23] The law for CSLI requests, 18 U.S.C. § 2703(d), has limits: the information sought must be material to an ongoing criminal investigation; state laws may stop state governments from obtaining a court order; and service providers may challenge the court order.

Also, the historical CSLI at issue in the present case raises fewer concerns than the real-time tracking at issue in *Jones*. Historical CSLI cannot chill associational and expressive freedoms because the government acquires the CSLI after the crime suspect has already associated and expressed.

Conversely, allowing a crime suspect's Fourth Amendment rights to prevent a third party from sharing information with the government would chill expressive freedoms. Third parties have First Amendment rights to disclose information to the government.[24] If crime suspects could stop third parties from doing so, then crime suspects could chill the expressive freedoms of third parties.

---

[23] *See City of Los Angeles v. Patel*, 135 S.Ct. 2443 (2015). (holding a hotel that objects to giving the police a guest list must be able to have an impartial court review the request).

[24] Orin Kerr, *Symposium: Carpenter and the Eyewitness Rule*, SCOTUSBLOG, (Aug. 4, 2017, 1:39 PM), http://www.scotusblog.com/2017/08/symposium-carpenter-eyewitness-rule.

Plus, crime hurts associational and expressive freedoms far more than acquiring the historical CSLI of crime suspects possibly could. In 2015, around 1,197,704 violent crimes occurred in the US.[25] The murder victims lost their associational and expressive freedoms. The assault victims suffered injuries (e.g., a broken jaw or worse) that hurt their associational and expressive freedoms. Also, the rape victims suffered trauma-related symptoms such as social withdrawal, suspicion of strangers, etc.[26]

Because violent criminals may be repeat offenders, applying the third-party doctrine to CSLI promotes associational and expressive freedoms. With the right tools, law enforcement may convict more violent criminals; fewer violent criminals may harm fewer crime victims; and fewer crime victims may suffer harms to their associational and expressive freedoms.

Finally, even if the government's acquisition of CSLI causes some chilling effects, the government's interest may outweigh the alleged chilling effects. When the government's interest relates to reducing criminal activity, this Court has tolerated some burdens on expressive and associational freedoms.[27]

---

[25] FBI, *Crime in the United States 2015*, tbl. 1, https://ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015/tables/table-1.

[26] Wash. Univ. in St. Louis, *Rape Trauma Syndrome*, https://rsvpcenter.wustl.edu/learn-more/rape-trauma-syndrome.

[27] *New York ex rel. Bryant v. Zimmerman*, 278 U.S. 63, 75-77 (1928) (upheld law that made KKK disclose members because of KKK's violent history); *Communist Party of the United States v.*

Even in a non-criminal case, based on the government's interest to inform voters, this Court upheld a campaign-finance law that required a group to disclose its donors, despite concerns that the disclosure rules would expose donors to retaliation.[28]

B. Cell Phone Users Have More Control Over Providing CSLI to Service Providers Than Crime Victims May Have Over Revealing Sensitive Information About Themselves.

This Court may hear arguments that people do not voluntarily provide CSLI to service providers,[29] but that is incorrect. On a short-term or a long-term basis, people can avoid providing CSLI by leaving their phones at home, by turning their phones off, and/or by using non-cellular devices.

Many crime victims lack the same control. If crime victims have disfiguring and visible injuries, then others may see their injuries and may sense their pain. Those crime victims have hardly any control over revealing sensitive information about themselves. If preserving the third-party doctrine reduces the number of crime victims that end up in that situation, then it is worth keeping around.

SACB, 367 U.S. 1, 90-105 (1961) (Communist Party had to disclose its members so government could monitor subversion).

[28] *Citizens United v. Federal Election Com'n*, 130 S.Ct. 876, 916 and 980-82 (2010).

[29] One irony is this Court may hear the argument from an attorney whose phone is off and not providing CSLI.

C. The Third-Party Doctrine Is More Important Than Ever in the Digital Age Because of "Substitution Effects"

According to Orin Kerr's "Substitution Effects" theory, the third-party doctrine deters criminals from substituting public parts of their crimes (e.g., stalking a victim in person) with private transactions for criminal acts (e.g., calling victim on the phone).[30]

The following examples show how new technologies make the third-party doctrine more important than ever in the digital age. One key issue is that artificial intelligence may reduce the number of human witnesses available to provide information to law enforcement. Because robots and/or driverless cars may replace human witnesses, the third-party doctrine may become more important than ever in the digital age to investigate crimes.

1. Bank Robbery

Figure 1 is from a video of a fictitious bank robbery.[31] Although the robber wears a mask, the robber's phone reveals his identity to the bank. The teller recognizes the robber's picture on her monitor.

---

[30] Blake E. Reid, Comment, *Substitution Effects: A Problematic Justification for the Third-Party Doctrine of the Fourth Amendment*, 8 J. ON TELECOMM. & HIGH TECH. L. 613, 615 n. 8 (2010) (citing Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 573, 576 (2009)).

[31] YouTube, *The Heist: Make Experience Your Business | Adobe Experience Cloud*, https://www.youtube.com/watch?v=_KOuliSqSJo.

Figure 1 – Bank Robbery

Figure 1 shows how information that people give to a third party may aid criminal investigations. The robber's phone pinged the bank's system. If the robber evades capture, then the third-party doctrine may help the police determine the robber's identity.

Treating low-tech and high-tech sources of information differently, under the third-party doctrine, would lead to absurd results. As a low-tech example, under the third-party doctrine, the law-abiding customers at the bank have no Fourth Amendment protection in the bank's records of their deposits.[32] The government could acquire those deposit records without a warrant. If the third-party doctrine does not apply to the ping that the bank receives from the robber's phone (i.e., a high-tech source), then the government would need a warrant for the bank's records related to the robber's identity.

Granted, the bank teller could identify the robber for the police; however, the bank teller of the

---

[32] *United States v. Miller*, 425 U.S. 435 (1976).

future may be a robot instead of a person.[33] A robot teller may not have a First Amendment right to identify the robber. Because artificial intelligence may reduce the number of human witnesses that can give information to police, the third-party doctrine may become more important than ever in the digital age to discourage and investigate unlawful activity.

2. Son of Sam Killer Using Ride Service

Forty years ago, the Son of Sam killer terrified New York City. Location information from a parking ticket solved that case. The police checked parking ticket records for witnesses, but found a ticket for the killer's car instead. Police noticed the killer's ticket because of his out-of-town address.[34]

What would happen today if the killer went to and from the murders using a ride service instead of his own car? The killer would not receive a parking ticket: the police would have to find him another way. If the third-party doctrine remains valid, then police could acquire route and passenger logs from the ride service without a warrant. Also, the killer's driver could reveal the killer's information to police.

---

[33] About 76% of bankers think artificial intelligence will be the main way banks interact with customers in 3 years. Accenture, *Banking Technology Vision 2017*, pp. 22-23, https://www.accenture.com/t20170322T205838Z__w__/us-en/_acnmedia/PDF-47/Accenture-Banking-Technology-Vision-2017.pdf#zoom=50.

[34] James Barron, *How a Son of Sam Detective Realized 'This Has Got to Be the Guy'*, N.Y. TIMES, Aug. 6, 2017, https://www.nytimes.com/2017/08/06/nyregion/son-of-sam-killings-david-berkowitz.html.

However, ride services are developing autonomous cars to replace human drivers.[35] Autonomous cars may lack First Amendment rights to speak with the police; thus, the third-party doctrine may become more important than ever in the future to deter and investigate illegal activity.

If the third-party doctrine goes away, then ride services may be more desirable for criminals. A wanted criminal driving his own car may worry about capture when the police or a license-plate reader (LPR) check his license plate. Many lower courts do not consider license-plate checks a search.[36]

In contrast, using an autonomous car through a ride service may be less risky. Even if the police check the license plate of the autonomous car, police would need to rely on the ride service, or another source, for passenger details. If the third-party doctrine goes away, then a killer like the Son of Sam might use an autonomous car through a ride service to lower his risk of capture.[37]

---

[35] *Uber not the only ride-hailing company with sights set on driverless cars*, AP, Sept. 18, 2016, https://www.cbsnews.com/news/uber-not-the-only-ride-hailing-company-with-sights-set-on-driverless-cars-lyft/.

[36] *See e.g.*, *United States v. Diaz-Castaneda*, 494 F.3d 1146, 1150 (9th Cir. 2007); *United States v. Walraven*, 892 F.2d 972, 974 (10th Cir. 1989).

[37] *See* Ariel Barkhurst, *Robbers turn to rental cars to avoid detection*, AZ SENTINEL, Apr. 12, 2012, http://articles.sun-sentinel.com/2012-04-03/news/fl-rental-cars-used-in-robberies-20120402_1_rental-cars-rental-vehicles-surveillance-cameras.

D. Laws Are the Best Way to Address Privacy Issues with the Third-Party Doctrine.

Justice Alito's concurrence in *Jones* states: "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative" because a "legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[38]

Congress put several safeguards in 18 U.S.C. § 2703(d). Under 18 U.S.C. § 2703(d), the government must have "reasonable grounds" but not "probable cause" to acquire non-content records like CSLI without a warrant or the third party's consent. The third-party may file a motion to modify or quash a court order for CSLI. A judge reviews the request. Also, many state laws prevent state governments from acquiring CSLI without a warrant.[39]

The time period of CSLI requested should be a factor in deciding whether the request complies with 18 U.S.C. § 2703(d), not whether the CSLI request violates the Fourth Amendment. If the CSLI relates to a long-term crime spree, then a court could decide the government has "reasonable grounds" to request a long-term period of historical CSLI.

---

[38] *Jones*, 132 S.Ct. at 964 (Alito J., concurring in judgement).

[39] ACLU, *Cell Phone Location Tracking Laws By State*, https://www.aclu.org/issues/privacy-technology/location-tracking/cell-phone-location-tracking-laws-state?redirect=map/cell-phone-location-tracking-laws-state.

Accordingly, this Court does not have to exclude CSLI from the third-party doctrine. People that want to change 18 U.S.C. § 2703(d) can pressure Congress to change the law, try to change the law in their state, or they can move to a state that requires a warrant for CSLI.

E. Markets Also Respond to Privacy Concerns from the Public.

Markets also respond to the public's privacy preferences. For example, in order to attract more corporate customers, Google no longer scans the emails of free-gmail users to target ad content.[40]

If some people want more privacy protection, then they may reward companies that provide people more privacy protection. They may pressure companies to challenge government § 2703(d) orders more often. Other people, however, might appreciate the benefits from CSLI. CSLI helps service providers find weak spots in their networks and offer new services (e.g., navigation services). Also, CSLI helps solve crimes, locate 911 callers, and rescue people.[41]

---

[40] Mark Bergen, *Google Will Stop Reading Your Emails for Gmail Ads*, Bloomberg Tech., June 23, 2017, https://www.bloomberg.com/news/articles/2017-06-23/google-will-stop-reading-your-emails-for-gmail-ads.

[41] M. Licea, *Serial killer with shipping container dungeon: My victims had it coming*, N.Y. Post, Sept. 9, 2017, http://nypost.com/2017/09/09/serial-killer-says-he-was-trying-to-save-woman-he-kept-in-shipping-container (CSLI helped find victim).

Markets also develop technologies that may provide more-targeted options for acquiring CPLI. For example, since cell towers cover a large area, the government may acquire over 150,000 phone numbers from a cell tower dump.[42] On the other hand, because Wi-Fi Access Points have a limited range (e.g., ~200 meters) and just detect devices with the Wi-Fi radio on,[43] the government may receive the non-content information of far fewer people from a Wi-Fi Access Point. In some situations, instead of a cell tower, a Wi-Fi Access Point may be an alternative source for CPLI.

II. The Past Use of Tracking Dogs to Determine Historical Location Information Is Analogous to Acquiring Historical CSLI.

There are similarities between using tracking dogs and gathering CSLI to determine historical location information. CSLI could be considered a digital scent trail of a mobile device. The digital scent trail is analogous to a person's scent trail with one exception: people can avoid leaving a digital scent trail by leaving their device at home; however, people cannot avoid leaving a physical scent trail.

---

[42] Nate Anderson, *How "cell tower dumps" caught the High Country Bandits – and why it matters*, ARS Technica, Aug. 29, 2013, https://arstechnica.com/tech-policy/2013/08/how-cell-tower-dumps-caught-the-high-country-bandits-and-why-it-matters.

[43] Libelium, *Meshlium Xtreme Technical Guide*, pp. 170, 174, and 177 (v. 7.3, July 2017), http://www.libelium.com/downloads/documentation/meshlium_technical_guide.pdf.

Before Benjamin Franklin was a delegate at the Constitutional Convention of 1787, he requested bloodhounds to help settlors find people accused of crimes.[44] Benjamin Franklin's past actions are relevant to colonial-era views about the government gathering historical location information in criminal investigations. Also, dogs have been used since at least the 1300s to follow the scent trail of crime suspects.[45] Accordingly, this Court's cases on scent-tracking dogs are relevant to whether the Fourth Amendment protects CSLI.

In *Florida v. Jardines*, this Court held that the government's use of a drug-sniffing dog on the front porch and curtilage of a home to detect marijuana in the home was a "search" in violation of the Fourth Amendment."[46] Otherwise, the Fourth Amendment does not prevent the government from using dogs to investigate areas beyond the curtilage. Without a warrant, dogs may check luggage at an airport, check a substance that has fallen from a parcel in transit, and check a car during a lawful traffic stop.[47]

---

[44] Kim C. Thornton, Bloodhounds 10 (1998); *see also* Nat'l Archives, *From Benjamin Franklin to Richard Jackson*, 25 June 1764, https://founders.archives.gov/documents/Franklin/01-11-02-0064 (Benjamin Franklin wanted bloodhounds to track native Americans accused of plundering and kidnapping).

[45] *See Florida v. Jardines*, 133 S.Ct. 1409, 1424 (2013) (Alito J., dissenting) ("Scottish law from 1318 made it a crime to 'disturb a tracking dog . . . pursuing thieves or seizing malefactors.").

[46] *Id.* at 1409.

[47] *Id.* at 1417 (citing *United States v. Place*, 103 S.Ct. 2637 (1983), *United States v. Jacobsen*, 104 S.Ct. 1652 (1984), and

The process for acquiring the CSLI is different from the Fourth Amendment violation in *Jardines*. In *Jardines*, the police used a dog to detect marijuana in a person's home, trespassed onto the person's property, and acted without a court order.[48] When the government acquires CSLI pertaining to a person, the government acts pursuant to a court order and acquires business records from a third party without trespassing onto the person's property.

III. People Lack a Reasonable Expectation of Privacy in Historical CSLI.

Generally, "a Fourth Amendment search occurs when the Government violates a subjective expectation of privacy that society recognizes as reasonable."[49] Also, trespasses upon a person, the person's house, the person's papers, and the person's effects count as a search.[50]

The Sixth Circuit's opinion provides several reasons why the government's acquisition of historical CSLI from a third party is not a search.[51]

Illinois v. Caballes, 125 S.Ct. 834 (2005)).

[48] *Id.* at 1413.

[49] *Kyllo v. United States*, 533 U.S. 27, 33 (2001).

[50] *Jones*, 132 S.Ct. at 950.

[51] *Carpenter*, 819 F.3d at 887-90 (holding the government's acquisition of CSLI was not a search because cell phone users (i) lack a property interest in historical CSLI, (ii) have lower privacy expectations in business records and routing (non-content) information, and (iii) should know their phone provides its location because of signal indicators and roaming charges).

However, there are more facts that bolster the Sixth Circuit's discussion on why people lack a reasonable expectation of privacy in historical CSLI. Because the present case concerns historical CSLI from December 2010 to April 2011, this brief discusses the facts known before December 2010 separately from the facts known today.

A. Before December 2010, Many Sources (e.g., FCC Rules, News, Manuals, Patents, and Movies) Informed the Public that Cell Phones Provided CSLI to Third Parties.

Before December 2010, most people knew or should have known that their cell phones provided CSLI to service providers.

First, based on Federal Communication Commission (FCC) rules, cell phone users around December 2010 should have expected no location privacy when they made 911 calls. By extension, cell phone users should have expected that the government could acquire CSLI for other purposes. In 1996, the FCC crafted rules to ensure wireless carriers would provide the location of wireless 911 callers to 911 call centers.[52] By October 1, 2001, the FCC started Phase II Emergency 911 (E-911) service requirements on wireless carriers.[53]

---

[52] See FCC, *FCC Report to Congress on the Deployment of E-911 Phase II Services By Tier III Service Providers*, p. 1 n. 3 (Mar. 23, 2005), https://apps.fcc.gov/edocs_public/attachmatch/DOC-257626A1.pdf.

[53] 47 C.F.R. § 20.18(e) to (h).

Effective December 31, 2005, the FCC's Phase II E-911 regulations require all new cell phones must be location-capable (i.e., have location-determining hardware and/or software for the wireless carrier to determine the cell phone's location for a 911 call).[54] The FCC's Phase II E-911 rules also set location-accuracy requirements that the wireless carriers must meet by certain target dates.[55]

Second, multiple sources explained that cell phones provided location information to others. Service contracts are one example.[56] Patents[57] and device manuals are other sources. An iPhone® user guide from 2009 discloses several phone features: the phone gives directions based on the phones current location; the phone provides location information during 911 calls; the phone tags photos with location information; and the phone lets users manage their location services.[58]

Even if the average person did not read FCC regulations, product manuals, or patents, news reports informed the public that cell phones provided location information to service providers.[59]

---

[54] 47 C.F.R. § 20.18(g)(1)(v).

[55] 47 C.F.R. § 20.18(h) (target dates are after January 18, 2011).

[56] U.S. Patent No. 8,073,460 col. 7 l. 7-30 (filed Mar. 29, 2007).

[57] *See e.g.*, U.S. Patent No. 5,519,760 abs. (filed June 22, 1994) and U.S. Patent No. 7,515,578 abs. (filed May 8, 2006).

[58] Apple, *supra*, note 9, at pp. 24, 51, 103, 114-19, and 144.

[59] *See e.g., Suspect in Kelsey Smith's Death Charged with Murder, Kidnapping*, FoxNews.com, June 7, 2007, http://www

Movies also notified the public. The Recruit, a 2003 spy thriller that grossed over $52 million in US sales, included a scene where CIA agents tracked the main character's location based on his cell phone.[60] Thus, by 2010, people knew or should have known that cell phones provided CSLI to third parties.

B. Today, People Have More Reasons to Know Their Cell Phones Provide CSLI to Third Parties.

People today have more reasons to know that their cell phones provide CSLI to third parties. With ride-sharing services, people can arrange for vehicles to pick them up at locations their phones provide. While people wait, their phones show the location of the driver's vehicle.[61] Applications help people find their lost or stolen phone.[62] Accordingly, it is hard to imagine how any cell phone users would be unaware that their cell phones provide CSLI to third parties.

.foxnews.com/story/2007/06/07/suspect-in-kelsey-smith-death-charged-with-murder-kidnapping.html ("[L]aw enforcement put search teams within a four-mile radius of where the body was found, based on the cell phone signals."); Ryan Hutchins, *Cell phone tracking software helps police, emergency workers*, NJ.com, Jun. 22, 2009, http://www.nj.com/news/index.ssf/2009/06/cell_phone_tracking_software_h.html.

[60] The Recruit (Touchstone Pictures 2003) (At the end, Dennis tells James, "You forgot to turn your cell phone off. That's how we tracked you: your cell phone.").

[61] *See e.g.*, Uber, *Ride*, https://www.uber.com/ride.

[62] *See e.g.*, Apple, *Find My iPhone*, https://www.apple.com/icloud/find-my-iphone.

Conclusion

For the foregoing reasons, the judgment of the Sixth Circuit Court of Appeals should be affirmed.

Respectfully submitted.

Michael Varco
Counsel of Record and
Amicus Curiae
P.O. Box 2548
Reston, VA 20195
(703) 635-9703
m_varco@yahoo.com

September 29, 2017